RAISECOM

www.raisecom.com

ISCOM2924GF CONFIGURATION GUIDE

15-06-2009

Legal Notices

Raisecom Technology Co., Ltd makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. **Raisecom Technology Co., Ltd** shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty.

A copy of the specific warranty terms applicable to your Raisecom product and replacement parts can be obtained from Service Office.

Restricted Rights Legend.

All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of **Raisecom Technology Co., Ltd.** The information contained in this document is subject to change without notice.

Copyright Notices.

Copyright ©2007 Raisecom. All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in Writing from **Raisecom Technology Co., Ltd.**

Trademark Notices

RAISECOM is the trademark of Raisecom Technology Co., Ltd.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows® XP is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of

Microsoft Corporation.

Contact Information

Technical Assistance Center

The Raisecom TAC is available to all customers who need technical assistance with a Raisecom product, technology, or, solution. You can communicate with us through the following methods:

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road, Haidian District, Beijing 100085

Tel: +86-10-82883305

Fax: +86-10-82883056

World Wide Web

You can access the most current Raisecom product information on the World Wide Web at the following URL:

http://www.raisecom.com

Feedback

Comments and questions about how the … system software works are welcomed. Please review the FAQ in the related manual, and if your question is not covered, send email by using the following web page:

http://www.raisecom.com/en/xcontactus/contactus.htm.

If you have comments on the … specification, instead of the web page above, please send comments to:

export@raisecom.com

We hope to hear from you!

CONTENTS

Release Notes

Date of Release	Manual Version	Software Version	Revisions

Preface

About This Manual

This manual introduces primary functions of the configuration management software for RC series products.

Who Should Read This Manual

This manual is a valuable reference for sales and marketing staff, after service staff and telecommunication network designers. For those who want to have an overview of the features, applications, structure and specifications of … device, this is also a recommended document.

Relevant Manuals

《Raisecom NView System User Manual》

《Raisecom Nview System Installation and Deployment Manual》

《… User Manual》

《… Commands Notebook》

Organization

This manual is an introduction of the main functions of … EMS. To have a quick grasp of the using of the EMS of … , please read this manual carefully. The manual is composed of the following chapters

Chapter 1 Overview

This chapter briefly introduces the basic function of …

Chapter 2 Configuration Management

This chapter mainly introduces the central site configuration management function of the ….

Chapter 3 Performance Management

This chapter focuses on performance management function of ….

Chapter 4 Device Maintenance Management

This chapter introduces the device maintenance management function of ….

Appendix A Alarm Type

The alarm types supported by ….

Compliance

The RC series products developed by Raisecom are strictly complied with the following standards as well as ITU-T, IEEE, IETF and related standards from other international telecommunication standard organizations:

YD/T900-1997 SDH Equipment Technical Requirements - Clock

YD/T973-1998 SDH 155Mb/s and 622Mb/s Technical conditions of optical transmitter module and receiver module

YD/T1017-1999 Network node interface for the Synchronous Digital Hierarchy (SDH)

YD/T1022-1999 Requirement of synchronous digital hierarchy (SDH) equipment function

YD/T1078-2000 SDH Transmission Network Technique Requirements-Interworking of Network Protection Architectures

YD/T1111.1-2001 Technical Requirements of SDH Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Receiver Modules

YD/T1111.2- 2001 Technical Requirements of SHD Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Transmitter Modules

YD/T1179- 2002 Technical Specification of Ethernet over SDH

G.703 Physical/electrical characteristics of hierarchical digital interfaces

G.704 Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels

G.707 Network node interface for the synchronous digital hierarchy (SDH)

G.774 Synchronous digital hierarchy (SDH) - Management information model for the network element view

G.781 Synchronization layer functions

G.783 Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks

G.784 Synchronous digital hierarchy (SDH) management

G.803 Architecture of transport networks based on the synchronous digital hierarchy (SDH)

G.813 Timing characteristics of SDH equipment slave clocks (SEC)

G.823 The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy

G.825 The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)

G.826 End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections

G.828 Error performance parameters and objectives for international, constant bit-rate synchronous digital paths

G.829 Error performance events for SDH multiplex and regenerator sections

G.831 Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)

G.841 Types and characteristics of SDH network protection architectures

G.842 Interworking of SDH network protection architectures

G.957 Optical interfaces for equipments and systems relating to the synchronous digital hierarchy

G.691 Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers

G.664 Optical safety procedures and requirements for optical transport systems

I.731 ATM Types and general characteristics of ATM equipment

I.732 ATM Functional characteristics of ATM equipment

IEEE 802.1Q Virtual Local Area Networks (LANs)

IEEE 802.1p Traffic Class Expediting and Dynamic Multicast Filtering

IEEE 802.3 CSMA/CD Access Method and Physical Layer Instruction
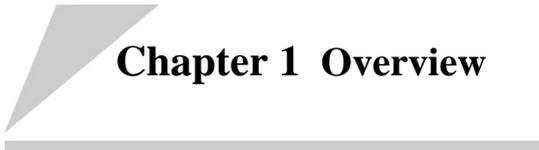
Chapter 1 Overview

1.1 Basic switch functions

➢ Mirror function: including the mirror that is from any port to one port, which is used for network data monitoring and analysis.
➢ System log: multiply log display mode is supported.
➢ System clock: SNTP time synchronization and manual configuration is supported.
➢ Task scheduling: with this function a certain command can be executed seasonally.

1.2 Layer-2 function

➢ MAC address table management: static MAC configuration and dynamic MAC learning are supported.
➢ Physical layer interface configuration: including rate and duplex mode configuration, 802.3x flowcontrol function and port enable/disable.
➢ Storm control: including broadcast, multicast and DLF frame control.
➢ Message relay and transmission: including the option of protocol messages or DLF message.
➢ Link aggregation: including aggregated link load balance.
➢ DHCP configuration: including DHCP Server, DHCP Relay and DHCP Snooping function, with the legal DHCP server user can get IP address automatically.
➢ ARP management: including static and dynamic ARP address table maintainnace.
➢ Loopback detection: aiming at the network trouble caused by Loop, it develops the robustness, fault tolerance and debugging ability of the network.
➢ VLAN configuration: including basic VLAN configuration, Q-in-Q and flexible Q-in-Q function.
➢ Shared VLAN: SVL mode is supported.
➢ RST configuration: IEEE 802.1w rapid spanning tree protocol is supported.
➢ MST configuration: IEEE 802.1Q multiply spanning tree protocol is supported.

1.3 Management function

➢ Basic management:
  ● Management using CONSOLE is supported;
  ● Remote management with TELNET is supported;
  ● Auto-configuration is supported, that is to download configuration files automatically from network management configuration server and realize network management configuration.
➢ SNMP configuration: SNMP v1, SNMP v2 and SNMP v3 is supported.
➢ RMON configuration: you can use different network agent and manage-station system to monitor network data, now RMON1, 2, 3, 9 groups are supported.
➢ Cluster management: with Raisecom cluster management function, network administrator is able to manage several switches using the public IP address of the main switch. Three protocols are included: RNDP, RTDP and RCMP.
➢ Bandwidth management function configuration: rate-limit based on port or VLAN is supported.
➢ ACL and network security configuration: multiply access list configuration is supported, you can sort and filter the packets according to the matching list.
➢ QoS function: specific traffic control, it offers end to end quality of service guarantee for user's service.
➢ OAM configuration: IEEE802.3ah is supported
➢ Extended OAM configuration: management and monitor remote devices with IEEE802.3ah OAM link, the main functions include: acquiring and configuring remote device attribution, downloading or uploading remote device files, managing extending OAM link state and statistics.
➢ Optical module digital diagnoses: SFP fault diagnose function is supported.

1.4 Protocols that the functions are based on

- RST: IEEE 802.1w;
- MST: IEEE 802.1Q;
- OAM: IEEE 802.3ah;
- Port flowcontrol function: IEEE 802.3x.

Chapter 2　Commands Line Usage

2.1　Introduction to commands line

Commands Line is the channel for the communication between subscribers and switches. In the commands lines, subscribers is able to monitor, control and manage the switches through configuring the corresponding commands. For better convenience, subscribers can edit shortcuts to use the commands, by the same time subscribers can examine the used commands through transferring the history. The commands line mode confines the way different subscribers use commands lines, where various commands line modes are offered. Subsribers can make certain configuration only in the corresponding mode.

2.2　Commands line usage configuration

2.2.1　Commands line mode configuration

Mode	Mode description	Access	Prompt	Out
Universal subscriber mode	Subscriber is allowed to configure the basic information and the parameter shown on the switch.	Login the switch and enter the user's name and password.	Raisecom>	**Exit** Withdraw from the current mode.
Subscriber privileges mode	Subscriber is allowed to configure the basic information of the switch, like system time and the name of the switch, except the operation information.	From universal subscriber mode, type **enable** and password.	Raisecom#	**Exit** Withdraw from the current mode.
Global configuration mode	Subscriber is allowed to configure all the operation parameters.	From subscriber privilege mode, type **config**	Raisecom(config)#	**Exit** Withdraw from the current mode.
Physical layer interface configuration mode	Subscriber is allowed to configure the Ethernet physical interface of the switch.	From global configuration mode, type **interface port portid**.	Raisecom(config-port)#	**Exit** Withdraw from the current mode.
Physical layer interface bulk configuration mode	Subscriber is allowed to range configure the parameter of the switch's Ethernet physical interface.	From global mode, type **interface port portid**.	Raisecom(config-range)#	**Exit** Withdraw from the current mode.

Three-tier interface configuration mode	Subscriber is allowed to configure the switch's three-tier Ethernet interface.	From global mode, type **interface port ip** id.	Raisecom(config-ip)#	**Exit** Withdraw from the current mode.
VLAN configuration mode	Subscriber is allowed to configure the VLAN operation parameters.	Enter **vlan**	Raisecom(config-vlan)#	**Exit** Withdraw from the current mode.
Class Map configuration mode	Subscriber is allowed to configure the given data flow.	From global configuration mode, type **class-map** class-map-name **[match-all | match-any]** command.	Raisecom(config-cmap)#	**Exit** Withdraw from the current mode.
Policy Map configuration mode	Subscriber is allowed to classify and package the data flow defined by class-map.	From global configuration mode, type **policy-map** policy-map-name command.	Raisecom(config-pmap)#	**Exit** Withdraw from the current mode.
Traffic classification configuration mode	Subscriber is allowed to configure the action of the date flow.	From policy map exec mode, type **class-map** class-name command.	Raisecom(config-pmap-c)#	**Exit** Withdraw from the current mode.
The cluster configuration mode	Subscriber is allowed to configure the cluster.	From global configuration mode, type **cluster** command.	Raisecom(config-cluster)#	**Exit** Withdraw from the current mode.
Access control list mapping table configuration mode	Subscriber is allowed to configure the access control list mapping table.	From global configuration mode, type **access-list-map** *<0-399> {permit | deny}* command.	Raisecom(config-aclmap)#	**Exit** Withdraw from the current mode.
Subscriber network mode	Subscriber is allowed to configure three-tier network setting, show the users' network information and network tools.	Form global configuration mode, type **user-network diagnostics.**	Raisecom(config-usrnet)#	**Exit** Withdraw from the current mode.
RIP configuration mode	Subscriber is allowed to configure RIP.	Form global configuration mode, type **router rip.**	Raisecom(config-router-rip)#	**Exit** Withdraw from the current mode.
OSPF configuration mode	Subscriber is allowed to configure OSPF.	From global configuration mode, type **router ospf**.	Raisecom(config-router-ospf)#	**Exit** Withdraw from the current mode.

2.2.2 Getting Help

Command	Description
help	Get a short system help both in English and in Chinese.
abbreviated-command-entry*?*	Get a list for all the available commands that match a particular string prefix (*abbreviated-command-entry*). For example: ISCOM> **en? english enable**
abbreviated-command-entry<*Tab*>	Makeup an incomplete command. For example. Raisecom#**show ser**<Tab> Raisecom#**show service**
?	List all the commands under this mode. For example Raisecom#**?**
command?	List all the key words and options for particular command with a short help information for it. Raisecom#**show ?**
command keyword ?	List the key words corresponding command For example Raisecom(config)#**ip***?* IP setting ip-access-list Define IP access control list

2.2.3   Using Editing Features

up arrow: last entered command

down arrow: next entered command

left arrow: move a character left

right arrow: move a character right

backspace: delete a character in front of the cursor

Ctrl+d: delete a character at the cursor

Ctrl+a: move the cursor to the beginning of the command line

Ctrl+e: move the cursor to the end of the command line

Ctrl+k: delete all the characters to the right the cursor

Ctrl+w: delete all the characters to the left of the cursor

Ctrl+u: delete the row all

Ctrl+z: exit from other modes to privileged mode

2.2.4　Command-line History

The switch records the latest 20 commands in the cache by default. User can use the following command to set the number of history commands that will be recorded:

Raisecom>**terminal history** *<0-20>*

Use **history** to show the history command.

2.2.5　The command-line Error

Error	Description	Getting help
Unknown command or in accurate For example Raisecom#**sh co** % "co" Unknown command.	Review the command needed.	
The command is not confirmed: For example Raisecom#**sh r** %"r" Unconfirmed command	Input the order that can not be recognized by the switch from the commands.	Add **?** for annotation and command. For example: Raisecom#**sh r** rate-limit: Rate control Rmon: Remote Network Monitoring (RMON) configuration Rndp: RNDP configuration Rtdp: RTDP configuration running-config: Running system configuration information
Command incomplete For example Raisecom#**show** % "show" Incomplete command.	The switch can not recognize the operation form the command, command that can be recognized is needed.	Add **?** for command and annotation. For example: Raisecom#**sh r** rate-limit:Rate control Rmon: Remote Network Monitoring (RMON) configuration Rndp: RNDP configuration Rtdp: RTDP configuration running-config: Running system configuration information

Chapter 3　System Function

3.1　File Management

3.1.1　Profile Management

The default configuration storage file name of the system is：**startup_config.conf**. The configuration storage file could be written into the flash file system through the command **write**, and the configuration information will be re-configured automatically the next time the system reboot. Use **erase** to delete the file. The configuration information file **startup_config.conf** could be uploaded to the server or downloaded to the system to replace the original configuration information, through FTP protocol with the command **upload** and **download**. Use **show startup-config** to show the configuration information in storage. Use **show running-config** to show the current configuration information in the system.

Command	Description
write	write the configuration file into the flash file system，and the configuration information in storage will be re-configured automatically after the system rebooting
erase	delete the file
show startup-config	the configuration information in storage
show running-config	The configuration information in the current system

3.1.2　BOOTROM file management

BOOTROM, boot of the switch, initialize the switch. User can upgrade BootROM file through FTP. BootROM file system is called **bootrom**(or **bootromfull**)in default cases. With the command **ftp file-name,** user can set these file system names.

When powered, the switch will run **BootROM** file first. When 'Press space into Bootrom menu…' is shown, user can enter **Bootrom** menu bar by pressing ENTER, and carry out the following operation:

'**?'** show all the commands available

'**h'** show all the commands available

'**v**' show the version of　**Bootrom**

'**b'** quick start executive command

'**T'** download configuration file through the switch ports

'N' set the MAC address

'R' reboot the switch

3.1.3 System File Management

The documents that keep the equipment running, like host software and configuration files, are kept in the storage devices.For the convenience and efficiency of user's managing the equipment, the equipment manage the documents in the way of Document System. The function of the document system contains catalog's creating and deleting, document's copying and display, and so on. In default cases, the document system will remind user for confirmation if the command may lose any data (like deleting or recovering files).

➢ With the command **upload** and **download,** program files could be uploaded to the server or downloaded to the system through the TFTP protocol or FTP protocol;
➢ Use **dir** to look over the system FLASH files;
➢ Use **show version** to look over the software version;
➢ Use **clock** to set system time;
➢ Use **logout** to exit the current system.

Command	Description
dir	To look over the system files
show version	To look over the software version
clock	To set system time
logout	exit

3.1.4 FPGA files management

FPGA(field programmable gate arrays) is the most integrated in Application Specific Integrated Circuit(ASIC). To accomplish user's logic, subscriber can re-configure the logical module and I/O module in FPGA, which can also be used on CPU's simulation. User's programming data to FPGA, stored in FLASH chip, could be uploaded to FPGA when powered and initialized. Online-programming is also available, making the system reconstructed online.

When powered, the FPGA chip will write the data in EPROM into programming ROM and get into working state after the configuration finished. When power off, FPGA will be empty and the logic inside is gone, thus FPGA could be repeated used. There is no special programmer for FPGA programming, the universal EPROM, PROM programmer can fit it. When the function of FPGA needs to be modified, only on piece of EPROM needs to be changed. So, by one FPGA different programming data brings different circuit function.

Command	Description
Upload *{system-boot/startup-configure/remote-fpga }* **ftp** *A.B.C.D username password filename*	Files are uploaded to server through FTP protocol A.B.C.D:IP destination address **username** server user name **password** user's password **filename** filename(o.0)
download *{system-boot/startup-configure/bootstrap/remote-fpga}* **ftp** *A.B.C.D username password filename*	By FTP protocol the files are downloaded to the system and replace the files before. A.B.C.D:IP destination address **username** server user name

	password user's password
	Filename filename(o.0)
upload *{system-boot|startup-configure|remote-f pga }* **tftp** *A.B.C.D filename*	Files are uploaded to server through FTP protocol **A.B.C.D**:IP destination address **Filename** filename
download *{system-boot|startup-configure|remote-f pga }* **tftp** *A.B.C.D filename*	Files are uploaded to server through FTP protocol **A.B.C.D**:IP destination address **Filename** filename

3.1.5 A typical configuration example

When subscriber has already have his/her own configuration files or new upgrade files, he/she can download the configuration files into the switch. To make it, subscriber should open the FTP software, like wftpd32.exe, and set user name, password and file path. As shown below, user name is wyj, password:123, the path of the configuration file is E:\TMP.
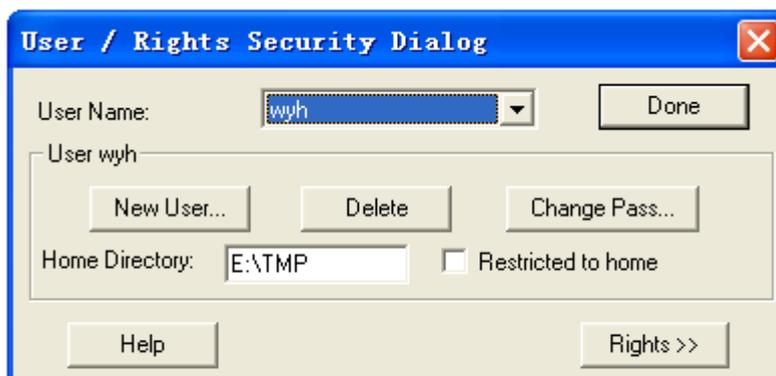
User uses serial line to connect the switch and PC, and connect the line to the switch port, as shown below. Open the terminal emulation program, such as **SecureCRT 5.1**. Take Console management as reference when using Console interface.
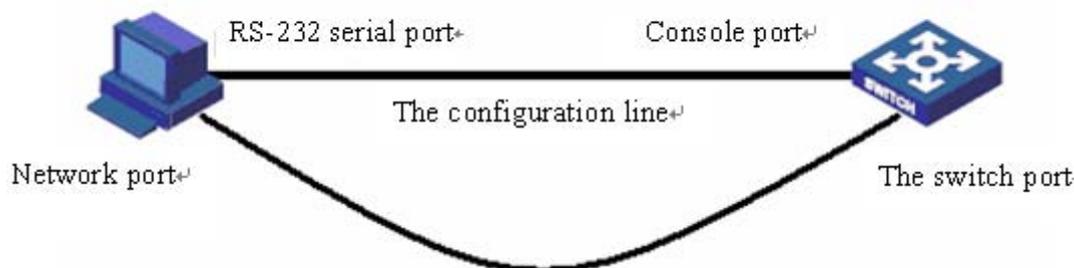
User can also use **Upload, download** to upload and download files from FTP. The connection line is shown as figure.

For example:

Using FTP to download system file **ROS_4.3.313.ISCOM2926.31.20080602** to the switch, user should set the switch IP address:20.0.0.10 first, then open the FTP software **wftpd32.exe** and set user name, password, and file path. Input **download** and select **system-boot**, input the host IP address: 20.0.0.10, user name,

password of the FTP software, and all the process is done.

Raisecom#*config*

Raisecom(config)#*interface   ip 0*

Raisecom(config-ip)#*ip address 20.0.0.10 1*

Set successfully

Raisecom(config-ip)#*exit*

Raisecom(config)#*exit*

Raisecom#**download** *startup-config ftp 20.0.0.221 wyh 123*

ROS_4.3.313.ISCOM2926.31.20080602

Waiting....Start

Getting from source ...Done

Writing to destination...Size 1754K / 1754K

Success!

When the files in switch need to be uploaded to the host, user can use TFTP to upload **startup-config** to the host. To do this, user should set the IP address 20.0.0.10 of the switch, then open the TFTP software **Cisco TFTP Server** to set the file path, input **upload**, host IP address 20.0.0.221, and upload the generated file name WW.

Raisecom#**config**

Raisecom(config)#**interface ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 1*

Set successfully

Raisecom(config-ip)#**exit**

Raisecom(config)#**exit**

Raisecom#**upload startup-config   tftp**   *20.0.0.221 ww*

Waiting....Start

Getting from source ...Done

Writing to destination...Size 1K / 1K

Success!

3.2 Switch Management

3.2.1 Console Management

Local control port management means using a console port of a terminal or a PC that is running terminal simulation program to configure and manage the switch. This management approach is out-of-band management, and needs no network for communication. Thus the console port can configure and manage the switch even if the network is not going on well.

Local management manage the switch by connecting the terminal and console program inside the switch.

To login in the Ethernet switch through the console port, the user's terminal communication parameter

configuration and the configuration of switch's console port should be consistent. The default configuration of the switch's console port is shown below

Attribution	Default value
Baud rate	9600bit/s
Flow control mode	No flow control
Check mode	No check
Stop bit	1
Data bit	8

First, connect the switch console port and the serial port of PC, and keep the PC online. As shown below,
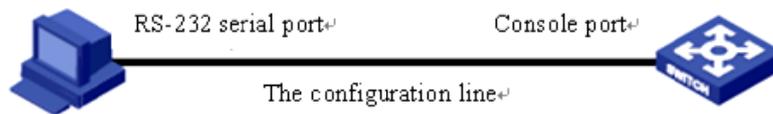
Then, run the terminal simulation program on PC, such as **SecureCRT 5.1**, as is shown below. Select the serial port connected with the switch port, and configure the terminal communication parameter as: baud rate 9600 bit/s, 8 data bits, 1 stop bit, no validation and flow control, serial interrupted default value 100ms.
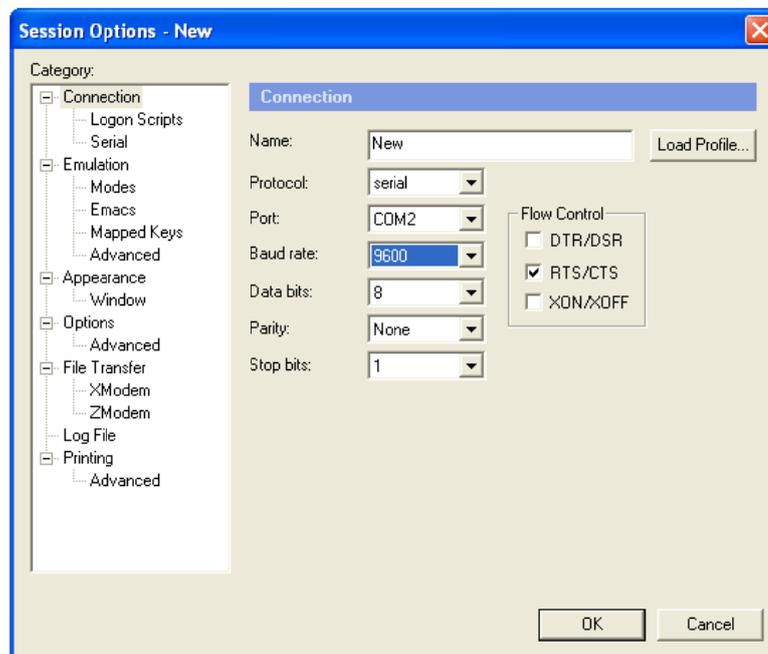
At last, download the system files to the switch and run it through console port. The calculation of the switch data can also be observed and controlled by computer.

3.2.2 Telnet management

The TELNET protocol aims at offering a communication mechanism which is generally universal, two-way and 8 byte available. Its main objective is letting terminal interface device and the process for terminal interact. In addition, as you can see, the protocol could be used in terminal communication (connection) and process to process communication (distributed computing).

A general thought: a telnet connection is a connection which is used to transfer TCP that contains TELNET control data.

TELNET protocol base on the following 3 ideas mainly: first, virtual network terminals; second, the principle of negotiating options; third, viewing the terminal and process as a balanced approach.

User can make remote management and maintenance through Telnet. Both switch client and telnet client need corresponding configuration so that user can login in the switch by Telnet.

When user login on a switch, the picture following shows the detail:
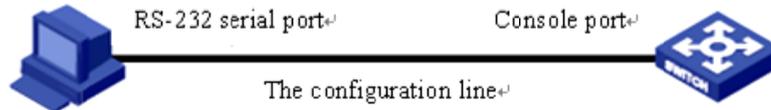
User can start TELNET services by command:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** 0	Enter IP port mode
3	**ip address** *A.B.C.D [A.B.C.D] <1-4094>*	Configure the IP address A.B.C.D: IP address [A.B.C.D]: subnet mask <1-4094>: vlan number
4	**exit**	Exit global configuration mode and enter enable mode
5	**telnet-server {accept|close|max-session}** *port-list*	Set telnet services port-list port list
6	**show telnet-server**	Show telnet configuration

3.2.3 SSH management

3.2.3.1 SSH default configuration

Function	Default value
SSH server status	Stop
Key-pair	No

3.2.3.2 SSH configuration

Before the server start key-pair have to be created. User manage command creating and key-pair deletion by key-pair. User use keys to create command and key-pair, before new key-pair is created, user must delete the key-pair that existed, because only one key-pair can be created on one equipment.

step	Command	Description
1	**config**	Enter global configuration mode
2	**key-pair generate** *KEYNAME* **rsa** *[modulus <768-2048>] [comment COMMENT]*	Create key pair KEYNAME key-pair name 768-2048 range of the module length COMMENT key-pair comment
3	**ssh server** *KEYNAME*	Start SSH server KEYNAME key-pair name
4	**exit**	Return to global configuration mode
5	**show key-pair KEYNAME**	Show key-pair information

User can use **no ssh server** to stop SSH server after the SSH server start.

The key-pair will be stored on the equipment automatically after successful creation, until user delete it or the equipment is formatted.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**key-pair destroy** *KEYNAME*	Destroy key-pair
3	**exit**	Return to global configuration mode
4	**show key-pair** *KEYNAME*	Show key-pair information

3.2.3.3 Monitoring And Maintaining

Command	Description
show key-pair KEYNAME	Show key-pair information
show ssh server	Show server configuration information
show ssh session	Show SSH dialog information

3.2.4 Cluster 'rcommand' Management

3.2.4.1 Cluster 'rcommand' Function Introduction

Using Raisecom cluster management function, network administrator is able to manage several switch through a registered IP address of the main switch. The main switch is command facility, while the other switches that are under administration will be member equipments. Member equipment needs not IP address setting usually, it is managed and maintained by manage equipment's redirection. The typical using environment is shown below:
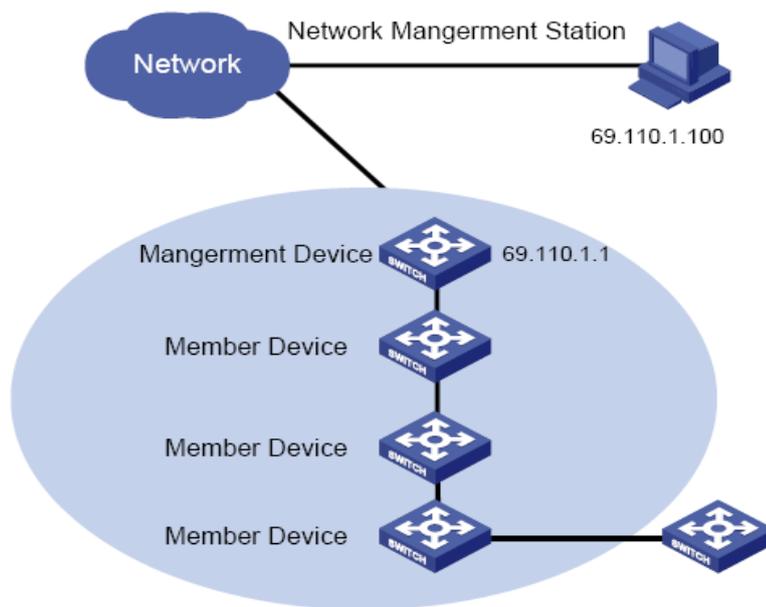
Cluster management contains three protocol: RNDP (Raisecom Neighbor Discover Protocol), RTDP (Raisecom Topology Discover Protocol) and RCMP (Raisecom Cluster Management Protocol). RNDP see to the facility neighbor discovery and information collection, RTDP see to collecting and handling all the network topology information, while RCMP see to the cluster member's joining, validation, deletion and so on. Among them, RTDP and RCMP communicate in cluster VLAN. So, appropriate configuration to VLAN2 is needed to make sure that RTDP and RCMP communicate normally, when there be facility that does not support Raisecom cluster management function between the two facilities that need cluster management.

Different roles form by the different degrees and functions of each switch in the cluster, but user can constitute a certain switch's role form configuration. The roles in cluster include supervisory unit, member unit and alternate unit.

Rcommand, like telnet, can login member switch on the command-line interface of the supervisor switch. Consult cluster management function about configuration and commands of cluster management.

3.2.5 NMS Management

NMS: Network Management System. It has 5 functions: alarming, performance, configuration, safety and accounting. In SNMP, NMS is the workstation running the client program. IBM NetView and Sun NetManager are the usual NMS stations in use. When SNMP Agent receives the query message Get-Request, Get-Next-Request, Get-Bulk-Request about MIB from NMS, Agent carry out **read** or **write** to MIB according to the message style, then create **Response** message according to the operation result and sent it to NMS as response.

On the other side, once SNMP Agent receives any change on facilities like normal/hot booting or anything unusual it will create a **Trap** massage and report it to NMS actively.

User can login the switch through NMS, manage and configure the switch by the Agent process on the switch. As shown below.
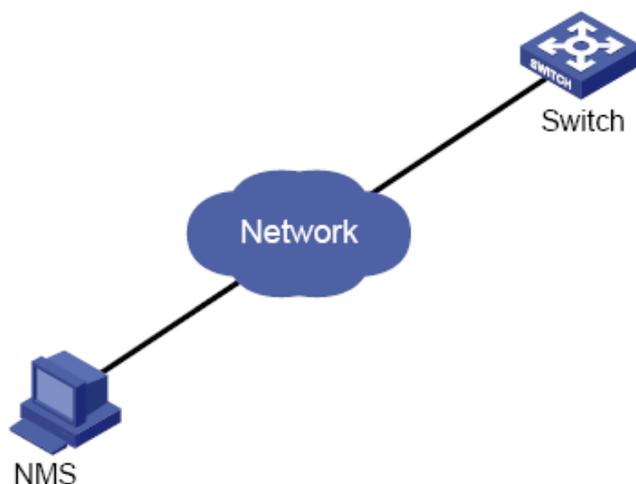
3.2.6 User Logging Management

User can login, configure and manage the switch by the following way:1, local login from Console port;2, local or remote login using Telnet through Ethernet port;3, login from NMS port. User's name and password is needed when logging, by default username is **raisecom**, password **raisecom**:

Setp	Command	Description
1	**user** *USERNAME* **password** { **no-encryption** | **md5** } *PASSWORD*	User login **USERNAME username**； **PASSWORD** password；
2	**user** *USERNAME* **privilege** *<1-15>*	User login privileges; **USERNAME** username； <1-15> user privileges grade；
3	**Write**	Save configuration information
4	**show user**	Show user information

3.2.7 Expended OAM Management

Expended OAM, by IEEE802.3ah OAM link, manage and monitor remote facilities. It contains 3 parts of function:1,aquire and set remote facilities;2, download and upload remote facility files;3, manage the expended OAM line state and stat.. Specific functions are as follows:

➢ Remote attribution acquirement: local facility can get remote facilities' attribution, configuration and statistics.

➢ Configuring remote facility basic function: local facility could configure remote facility function by expending OAM, including host name, port enable/disable, port speed duplex, port bandwidth, failover and so on.

➢ Configuring remote facility management parameter: configure network administration parameter for remote facility that support SNMP network administration, like IP address, gateway, group parameter and VLAN management, and carry out comprehensive network management through SNMP protocol.

➢ Remote TRAP: when remote facilities find **LINK UP/DOWN** port, the remote port will inform local port by sending expended OAM **notification** frame, then the local port will send remote TRAP alarm to network administrator.

➢ Expended remote end loopback: the local end is able to manage remote fiber port inner loop

function, and set the loopback data to decide if CRC needs re-computing.
- ➢ Resetting remote facilities: orders from local end is able to reset or reboot remote facilities.
- ➢ Other remote facilities' function management: as remote facilities increases, local facility can manage more remote end functions by expend OAM protocol, like SFP, Q-in-Q, virtual line diagnoses and so on.
- ➢ Downloading remote end files: remote end files could be downloaded to remote facilities directly from FTP/TFTP server, another way is downloading them from server to local end, then to the remote facilities.
- ➢ Uploading remote end files: remote end files could be upnloaded to remote facilities directly from FTP/TFTP server, another way is uploading them from server to local end, then to the remote facilities.
- ➢ Expended OAM line stat. and function management.

Expended OAM network is shown as below. Local switch MASTER:ISCOM2828F; remote end SLAVE: RC552-GE.
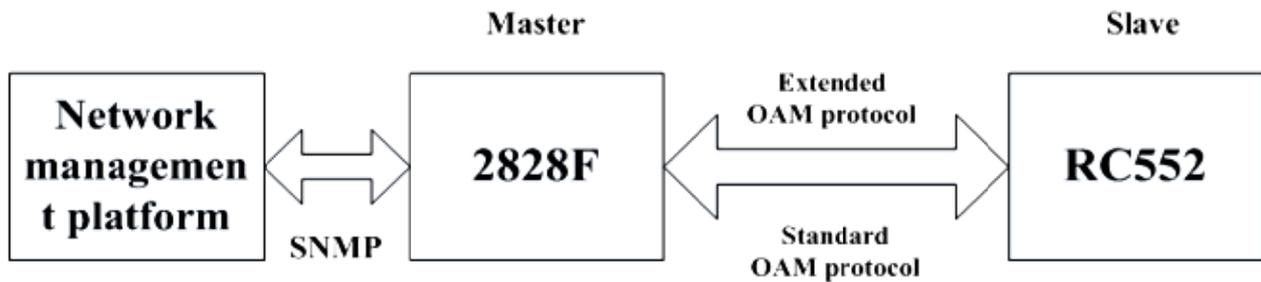
Notice: The expended OAM line could be established only between the local facility and remote facility, that is to say, the facility on each end must be OAM active mode and OAM passive mode respectively.

3.3 Keepalive Function

3.3.1 The Introduction To Keepalive Principle

To find out the facility out of order in time, user needs to acquire the facility information periodically to see if the facility is available and the basic facility information. Users can receive the state of **Keepalive Trap** information collection facility from NMS periodically without any operation. Keepalive module send TRAP periodically to NMS about the basic information of facilities, including facilities' name, facilities' OID, the hardware and software version, MAC address and IP address.

Keepalive module send **keepalive trap** that contains the basic information of the switch to the network administration station, so that the network administration station could find the switch in a short time.

3.3.2 Keepalive Default Configuration

Function	Default value
keepalive trap switch	On
Keepalive alternation	300 seconds

3.3.3 Keepalive Configuration

By default, KEEPALIVE is open on the switch, and the switch send KEEPALIVE trap periodically. By

carrying out the following command in global configuration mode, KEEPALIVE can be set OPEN, CLOSE and PAUSE. If it is CLOSE, the configuration can be loaded. And if it is PAUSE, the configuration can not be saved, the configuration is still default after reboot.

Step	Command	Description
1	**config**	Enter configuration mode
2	**interface ip** *0*	Enter IP port mode
3	**ip address** *A.B.C.D [A.B.C.D]* *<1-4094>*	Configure the IP address of the switch *A.B.C.D*: IP address *[A.B.C.D]*: subnet mask *<1-4094>*: vlan number
4	**exit**	Quit global configuration mode and enter privileged EXEC mode
5	**snmp-server host** *A.B.C.D* **version** *3* *{ noauthnopriv | authnopriv } NAME [udpport <1-65535>] [bridge] [config] [interface] [rmon] [snmp] [ospf]*	Configure SNMPv3 Trap the destination host *A.B.C.D*: IP address *NAME*: SNMPv3 team name *<1-65535>*: the UDP port number which the destination use to receive TRAP
6	**snmp-server keepalive-trap interval** *<120-28800>*	Set he interval time fo the switch sending KEEPALIVE-TRAP to SNMP network administration station *<120-28800>*: the interval range, the unit is second
7	**snmp-server keepalive-trap** {*enable|disable|pause*}	Start, close, pause sending keep alive trap
8	**exit**	Return to privileged EXEC mode
9	**show snmp config**	Show basic SNMP configuration

3.3.4 Monitoring And Maintenance

Show is used to show switch the operation and configuration for maintenance and monitoring. To do this, the following **show** command is available:

Command	Description
show snmp config	Show the basic configuration of SNMP

3.3.5 An Example Of Typical Configuration
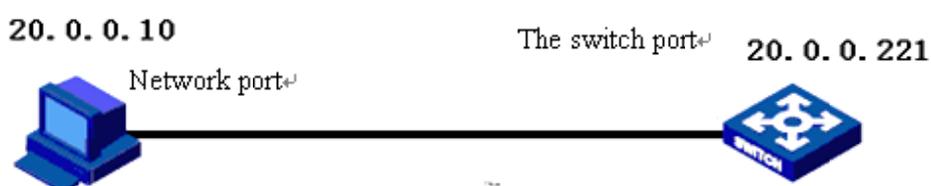
As is shown above, set the IP address as 20.0.0.10 first, then configure the SNMPv2c Trap destination host

address: add a **host_1** host address, username public, SNMP version v2c, all trap, set the interval time 500S of the switch sending **keepalive-trap** to SNMP network administration station, open **keepalive trap**, show basic SNMP information at last.

Raisecom#config

Raisecom(config)# **int ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**snmp-server host** *20.0.0.221* **version 2c public**

Raisecom(config)#**snmp-server keepalive-trap interval** *500*

Raisecom(config)#**snmp-server keepalive-trap** *enable*

Raisecom(config)# **show snmp config**

3.4 Task Scheduling Function

3.4.1 The Introduction To Task Scheduling Function Principle

The function is to carry out certain command periodically and maintain the switch configuration function seasonally. By configuring time list a time attribution list could be found, including start time , periodically time and end time. There are two kinds of time attribution, one begins when the switch starts, which is relative time; the other is the normal time, including year, month, day and so on, which is absolute time.

3.4.2 Task Scheduling Configuration

1. Setting task schedule:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**schedule-list list-no start {up-time days time** *[every days time [stop days time]]* **|date-time** *date time [every {day|week|days time} [stop date time]]*}	Add or modify **sechedule-list** table. The command set the beginning time and end time of scheduling task, and the cycling interval. **list-no**: the range of scheduling list number<0-99>; **days time**: from the start-up time start, it is relative time; input format **days:** *<0-65535>*, **time: HH:MM:SS** such as 3 3:2:1 date time: the calculation of time is in accordance with the system data，it is absolute time; input format: **MMM-DD-YYYY HH:MM:SS**: like jan-1-2003 or 1-1-2003, the range of **YYYY** is from 1970 to 2199.
3	**command-string** *schedule-list* **list-no**	Add the commands that support **schedule-list** to the scheduling list. **command-string**: command string. **list-no**: list number range<0-99>

| 4 | show schedule-list | Show **schedule-list** configuration。 |

3.4.3 Monitoring And Maintaining

Command	Description
show schedule-list	Show schedule-list configuration

3.4.4 Typical Configuration

First, add a **schedule-list** table, **List number:** 1, the beginning time is Feb-2-2004 0:0:0 according to system date, and perform every six days, while the terminal time is Feb-2-2005. Then, add the commands that support **schedule-list** to schedule list, and show the **schedule-list** configuration at last.

Raisecom#**config**

Raisecom(config)#**schedule-list** *1* **start date-time** *Feb-2-2004 0:0:0 every 6 0:0:0   stop Feb-2-2005 0:0:0*

Raisecom(config)#**storm-control dlf schedule-list** *1*

Raisecom(config)#**exit**

Raisecom# **show schedule-list**

3.5 Fault Location

3.5.1 Fault Location Principle

When anything abnormal happened in the system, fault location can be carried out by examining the facilities' running information, which includes the following contents:

- ➢ RAM using;
- ➢ port driver;
- ➢ process and stack state;
- ➢ port UP/DOWN statistics;
- ➢ the information needed for fault location.

3.5.2 Memory Show

Command	Description
show memory	Show the memory state

3.5.3 Port Driver Memory Pool Show

Command	Description

show buffer [port *<1-26>***]**	Show the port driver pool state; *<1-26>*: port range

3.5.4 Port UP/DOWN History

Command	Description
show diags link-flap	Show the UP/DOWN statistics

3.5.5 Fault Location Information Summarize Show

Command	Description
show tech-support	Show the fault location information summarize .

This command shows the information summarize for fault location, including:

- ➢ version (**show version**)
- ➢ running configuration information (**show running-config**)
- ➢ current CPU utilization (**show cpu-utilization**)
- ➢ memory usage (**show memory**)
- ➢ port driver pool usage (**show buffer**)
- ➢ processes (**show processes**)
- ➢ files in flash (**dir**)
- ➢ current system time (**show clock**)
- ➢ interface port state (**show interface port**)
- ➢ interface port statistics (**show interface port statistics**)
- ➢ port **UP/DOWN** statistics (**show diags link-flap**)
- ➢ SNMP statistics (**show snmp statistics**)
- ➢ spanning-tree in general (**show spanning-tree**)
- ➢ vlan statistics (**show vlan static**)
- ➢ ARP (**show arp**)
- ➢ trunk (**show trunk**)
- ➢ TCP link state

3.6 Ping Diagnose Function

3.6.1 Ping Principle

Ping is the most frequently-used command for troubleshooting, which is usually used to test if the link between the two hosts works. **Ping** is carried out by ICMP ECHO messages usually. It is made of ICMP reply and questioning messages, and if the network works well a reply messages will be received.

Ping can also be carried out through other paths, such as UDP, TCP and SNMP. In general, almost all the requests/replies can be used to acquire reply time. Usually, the ways except ICMP ECHO is used to settle the problem that some routers' no response or low response priority leads to the wrong answering time.

3.6.2 Ping Configuration

Test if the remote host is accessible.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** 0	Inter ip port mode
3	**ip address** *A.B.C.D* *[A.B.C.D] <1-4094>*	Configure the ip address on the switch A.B.C.D IP address [A.B.C.D] subnet mask <1-4094> vlan number
4	**exit**	Exit global configuration mode and enter privileged EXEC mode
5	**exit**	Exit privileged EXEC mode
6	**ping** *Ipaddress* [**count** *NumPktsRe*] [**size** *SizeofIcmpeChPkt*] [**waittime** *PktTimOut*]	Test if the remote host is accessible *Ipaddress*: test the IP address A.B.C.D NumPktsRe: *Number of packets to receive* specify the package number before the **ping** program ends <1-65535> *SizeofIcmpeChPkt*: *Size of icmp echo packet* specify the size of the ICMP answering message<1-4096> *PktTimOut*: *Packet timeout in seconds* specify the time-out time of **ping** waiting for answer <1-100>, the unit is milliseconds

3.6.3   Typical Configuration Example

As is shown below, the host connects the switch with cable. User can confirm if the connection works through the command **ping**, while the switch is also able to transfer data to the host through **ping**.

1. Set the switch IP address as 20.0.0.10, the connection IP address as 10.168.0.221, the number of messages sent is 3, the message size is 100, waiting time 3. Because the destination IP address goes against the PC IP, the connection does not work.

Raisecom#**config**

Raisecom(config)# **int ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**exit**

Raisecom#**ping** *10.168.0.221* **count** *3* **size** *100* **waittime** *3*

Type CTRL+C to abort.

Sending 3, 108-byte ICMP Echos to 10.168.0.221 , timeout is 3 seconds:

UUU

no answer from 10.168.0.221

Ping unsuccessfully

2. connect PC, the IP address is 20.0.0.221, set the switch IP 20.0.0.10, connect success will be shown.

Raisecom#**config**

Raisecom(config)# **int ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**exit**

Raisecom#**ping** *20.0.0.10* **count** *3* **size** *100* **waittime** *3*

Type CTRL+C to abort.

Sending 3, 108-byte ICMP Echos to 20.0.0.221 , timeout is 3 seconds:

!!!

Success rate is 100 percent(3/3)

round-trip (ms)   min/avg/max = 0/10/32

3.7 Tracerout Diagnose

3.7.1 Traceroute Principle

Traceroute, like **ping,** is a useful way of network management, which is use to find the route that the routers and lines that the message actually passes.

L3 Traceroute is carried out by sending a group of incremental TTL probe packets. Probe packets work in the form of UDP or ICMP Echo. If only TTL>0, or a ICMP will be returned per hop to the destination. From this message the RRT of per hop on the way to destination.

3.7.2 Traceroute Configuration

Before L3 Traceroute is used, the IP address and default gateway of the switch need configuration first.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** *0*	Enter IP configuration mode
3	**ip address** *A.B.C.D [A.B.C.D]* *<1-4094>*	Configure the IP address of the switch *A.B.C.D*: IP address *[A.B.C.D]*: subnet mask *<1-4094>*: vlan number
4	**exit**	Quit global configuration mode and enter privileged EXEC mode
5	**ip default-gateway** *A.B.C.D*	Configure the default gateway

		A.B.C.D: gateway number
6	**show int ip**	Show IP configuration
7	**show running**	Show default gateway configuration
8	**traceroute** *A.B.C.D* [**firstTTL** *<1-255>*] [**maxTTL** *<1-255>*] [**port** *<1-65535>*] [**waittime** *<1-60>*] [**count** *<1-10>]*	traceRoute show the route to destination *A.B.C.D*: IP address *firstTTL*: initialize TTL value *maxTTL*: maximize TTL value *<1-255>*: TTL value range *<1-65535>*: Port number range *<1-60>*: waiting time range *<1-10>*: count value

3.7.3   Typical Configuration Example

Example: set the IP address as 10.0.0.8, default gateway 10.100.0.1, trace the route to 58.63.236.42(www.sina.com.cn)

Raisecom#**config**

Raisecom(config)# **int ip** *0*

Raisecom(config-ip)#**ip address** *10.0.0.8 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**ip default-gateway** *10.100.0.1*

Raisecom(config)#**exit**

Raisecom#**Tracing** *the route to 58.63.236.42*

Type ctrl+c to abort.

1   10.0.0.1   10 ms   10 ms   10 ms

2   192.168.101.5   3 ms   3 ms   73 ms

3   192.168.101.5   10 ms   10 ms   10 ms

4   202.96.4.81   18 ms   16 ms   19 ms

5   202.106.228.177   9 ms   5 ms   12 ms

6   202.106.228.5   10 ms   8 ms   9 ms

7   202.96.12.25   7 ms   8 ms   5 ms

8   219.158.11.66   24 ms   20 ms   10 ms

9   202.97.15.57   101 ms   101 ms   126 ms

10   202.97.60.185   218 ms   222 ms   205 ms

11   202.97.40.58   119 ms   112 ms   113 ms

12   219.136.246.134   118 ms   142 ms   131 ms

13   219.136.246.6   138 ms   135 ms   110 ms

14   58.63.232.46   103 ms   115 ms   105 ms

15   58.63.236.42   199 ms   205 ms   197 ms

Trace complete.

3.8 Telnetd

3.8.1 Telnetd Principle

Telnet is the standard protocol and main way of remote login, which offers the ability of working on the local machine for remote host. The telnetd module in ROS4.0 implements the function of telnet server, letting telnet remote client login the facility so that it could be logged in and managed by telnet client.

3.8.2 Telnet Default Configuration

Function	Default value
Telnet server up-ling limit	5
telnet server link physical port	All the ports

3.8.3 Telnetd Configuration

1. Close telnet configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**telnet-server close**	Telnet server close
	terminal-telnet <1-5>	<1-5> end telnet dialog number
3	**exit**	Return to privileged EXEC mode
4	**show telnet-server**	Show current telnet server configuration

2. Set the telnet server linking upper-limit

Step	Command	Description
1	**config**	Enter global configuration mode
2	**telnet-server max-session** *<0-5>*	Set the telnet server linking upper-limit <0-5> linking number
3	**telnet-server accept** *port-list (all|{1-MAX_PORT_STR})*	Set the available port of the telnet server port-list: port list All: all the ports MAX_PORT_STR: port upper limit
4	**exit**	Return to privileged EXEC mode
5	**show telnet-server**	Show the current configuration of the telnet server
6	**Show information port**	Show information port

3.8.4   Typical Configuration Example

Set the linking upper limit of the telnet server as 3, open the available ports of Telnet server and show the current configuration.

Raisecom#**config**

Raisecom(config)#**telnet-server max-session** *3*

Set successfully

Raisecom(config)#**telnet-server accept port** *3*

Raisecom(config)#**exit**

Raisecom#**show telnet-server**

Max session: 3

Accept port-list: 1-26

3.9   Watchdog Function

3.9.1   Watchdog Principle

By configuring the watchdog software, the system program going into endless loop can be avoided, and the system stability will be better.

3.9.2   Configure Watchdog

Enable and Disable watchdog

Step	Command	Description
1	**watchdog** *{enable|disable}*	Enable: open watchdog Disable: close watchdog
2	**show watchdog**	Show watchdog state

3.9.3   Typical Configuration Example

Open watchdog and show the state

Raisecom#**watchdog** *enable*

Set successfully

Raisecom#**show watchdog**

Watchdog function: Enable

Chapter 4 Mirror Function

4.1 Local Port Mirror Function Principle

Mirror function is to copy some messages the appointed destination port from the appointed source port, while the normal message transmission works well. With this function, exchange equipment user can monitor the message delivering and receiving of a certain port, and analyse the network situation or defaults.
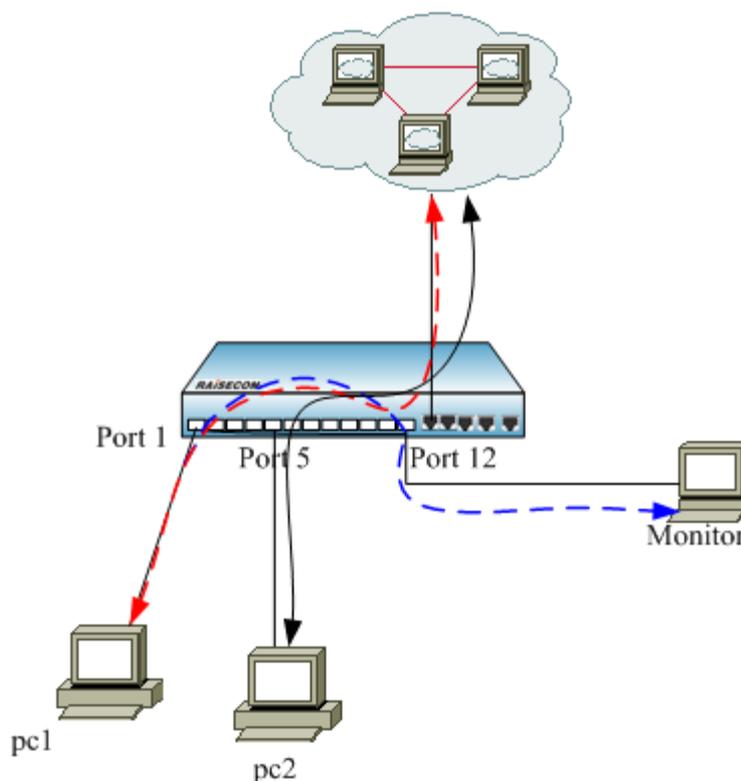
Mirror Function

Consult 1-1 as the principle.

PC1 and PC2 connect internet through port 1 and port 5 of the exchange equipment. When we need to monitor the data from PC1, we need to appoint the port 1 of the facility on connection as the mirror source port, and enable the mirror function of the receiving port message, then appoint monitoring port 12 as the destination port. When the data message from PC1 enters the exchange equipment, it will transfer the message and copy the message to the mirroring destination port (port 12). The monitoring equipment connected with the mirror destination port can receive the messages that is mirrored and make analysis.

4.2 Local Port Mirror Function Configuration

4.2.1 The Default Configuration

Function	Default value
Port mirroring	Disable
Mirror source port	Example
Mirror destination port	Port 1

4.2.2 Local Port Mirroring Function configuration

The traffic of source port will be copied to monitor port, so that network administrators can analyze the network.. Port 1 is monitor port by default, the source port and the monitor can not be same port.

When the mirror function go into effect, the message from I/O mirror ports will be copied to the monitoring port. The mirroring rules are set when the mirror ports are configured: both, ingress and/or egress. Also, the port can not be set as mirror port when it has already been set as monitoring port.

Only after the mirror function is enabled can the other configurations go into effect.

Step	Command	Description
1	config	Enter global configuration mode
2	**mirror** { **enable** | **disable** }	Enable/disable the mirror function
3	**mirror monitor-port** *port_number*	Set the monitor port. *port_number* is physical port number, range is 1-26.
4	**mirror source-port-list**{ **both** *port-list* | **ingress** *port-list*| **egress** *port-list* | **ingress** *port-list* **egress** *port-list*}	Set source port list, and appoint the corresponding ingress/egress *port-list* is the physical port list, use ',' and '- to carry out multi-port input.
5	**exit**	Quit global configuration mode and enter privileged EXEC mode.
6	show mirror	Show mirror configuration

Notice:

➢ The mirroring messages also need to comply the VLAN configuration transmission rules of the port.

➢ There can be more than one mirroring port, but only one monitoring port is allowed. Mirror function is disabled by default.

With configuration command **no mirror source-port-list**, the mirroring port that has been configured can be deleted.

With configuration command **no mirror all**, all the mirroring configuration can be deleted.

4.2.3 Monitoring And Maintaining

The command to show the port mirroring function

Command	Description
show mirror	Show the port mirroring function

4.2.4 Typical Configuration Example

Set port 26 as the monitoring port, **ingress** port 5-8, **egress** port 7-12

Raisecom #**config**

Raisecom (config)#**mirror enable**

Raisecom (config)#**mirror monitor-port** *26*

Raisecom (config)#**mirror source-port-list ingres**s *5-8* **egress** *7-12*

Raisecom (config)**#exit**

Raisecom #**show mirror**

Mirror: Enable

Monitor port: 26

-----------the ingress mirror rule-----------

Mirrored ports: 5-8

-----------the egress mirror rule-----------

Mirrored ports: 7-12

4.3 Mirroring Data Control Function

4.3.1 Mirroring Data Control Default Configuration

Function	Default value
Mirror destination port halting the not-mirroring data	Disable
Mirror source port ingress message split-flow number	1
Mirror source port ingress message filter source MAC address	0000.0000.0000
Mirror source port ingress filter destination MAC address	0000.0000.0000
Mirror source port egress message split-flow number	1
Mirror source port egress message filter source MAC address	0000.0000.0000
Mirror source port egress message filter destination MAC address	0000.0000.0000

4.3.2 Mirror Data Control Configuration

With the following commands, the mirror data can be within transmission control:

Step	Command	Description
1	**config**	Enter global mode
2(optical)	**mirror block-non-mirror** [*enable*/*disable*]	Configure the mirror destination port to enable/disable the filter function for the not-mirror messages
3(optical)	**mirror** [*ingress*/*egress*] **divider** <*1-1023*>	Configure after how many messages a packet is sent to the mirror pot from the source mirror ports' mirror data

4(optical)	**mirror** *[ingress | egress] filter {source | destination} HHHH.HHHH.HHHH*	For the source mirror port, configure to which MAC address the mirror function is closed
5	**exit**	Quit global configuration mode and enter privileged EXEC mode
6	**show mirror**	Show mirror configuration

Notice:

These commands are all configured in global configuration mode，and once the configuration is carried out it will affect all the source ports and destination ports.

The source and destination filter can configure only one MAC address.

4.3.3 Monitoring And Maintaining

Show the commands of mirror function

Command	Description
show mirror	Show mirror configuration

4.3.4 Typical Configuration Example

To figure 1-1, if there is too many data messages for port 1 to receive, and reducing the packets number for the monitoring facility is needed, it is supposed to do the following configuration:

Raisecom #**config**

Raisecom (config)#**mirror enable**

Raisecom (config)#**mirror monitor-port** *12*

Raisecom (config)#**mirror source-port-list ingres**s *1*

Raisecom (config)# **mirror ingress divider** *200*

Raisecom (config)#**exit**

Raisecom #**show mirror**

Mirror: enable

Monitor port: 12

Non-mirror port: Not block

-----------the ingress mirror rule----------

Mirrored ports: 1

Filter rule: All

Divider: 200

MAC address: 0000.0000.0000

-----------the egress mirror rule-----------

Mirrored ports: --

Filter rule: All

4.4 VLAN Stream Mirror Function

Function	Default value
VLAN mirror port list	Empty
VLAN mirror VLANlist	Empty

4.4.1 Configure VLAN Stream Mirror Function

VLAN included in the VLAN stream mirror VLAN list, can be mirrored to the monitoring port if the entrance to the switch exists in the VLAN stream mirror port list.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mirror source-vlan portlist** *portlist*	Configure VLAN stream mirror port list *portlist*: port list. can make multi-port input through the connector ',' and '-'.
3	**mirror source-vlan vlanlist** *vlanlist*	Configure VLAN stream mirror VLAN list *vlan list*: VLAN list, can make multi-VLAN ID input through the connector ',' and '-'.
4	**exit**	Quit global configuration mode and enter privileged EXEC mode
5	**show mirror**	Show mirror configuration

Use **no** to clear up VLAN stream mirror port list, or **no mirror source-vlan portlist.**

Use **no** to clear up VLAN stream mirror VLAN list, or **no mirror source-vlan vlanlist.**

Notice:

- Use the same command to enable VLAN stream mirror function and enable local port mirror function.

- The same monitoring port is used for VLAN stream mirror function and local port stream mirroring function.

- The local port mirror command **no mirror all** is compatible, but when it is executed, VLAN stream mirror function is no longer valid.

- VLAN that has not been created can be added to VLAN stream mirror VLAN list, but will not be valid until it has been created and active.

4.4.2 Monitoring And Maintaining

Show the command of VLAN stream mirror function:

Command	Description
show mirror	Show mirror configuration

4.4.3 Typical Configuration Example

➢ Aim

Configure the monitoring port as 5, mirror the messages from VLAN 10, port 2 to the monitoring port.

➢ Configuration step

Step 1: enable mirror function, and configure monitoring port 5

Raisecom (config)#**mirror** *enable*

Raisecom (config)#**mirror monitor-port** *5*

Step 2: configure VLAN stream mirror VLAN list

Raisecom (config)#**mirror source-vlan** *vlanlist 10*

Step 3: configure VLAN stream mirror port list

Raisecom (config)#**mirror source-vlan** *portlist 2*

Show the result:

Raisecom#**show mirror**

Mirror: Enable

Monitor port: 5

--------------the ingress mirror rule----------------

Mirrored ports: --

VlanMirrored ports: 10

VlanMirrored Vlans: 2

--------------the egress mirror rule--------------

Mirrored ports: --

Chapter 5 Port Rate Management

5.1 Port rate limiting and shaping principle

Line rate means rate limiting based on ports, which restricts the overall rate of the ports' receiving and sending messages. Line rate uses token bucket to control the rate. If some port of the facility is in rate limit, all the messages received or sent by the port need to be handled by token bucket. If there is enough token in token bucket, then messages can be received or sent, or it will be abandoned.
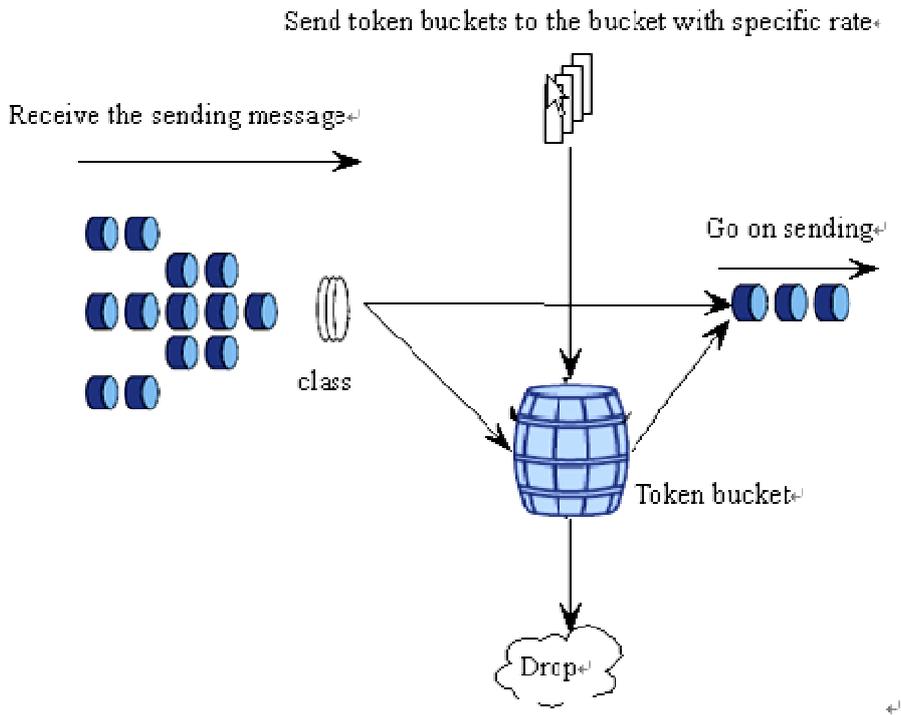
Fig-1 line rate process

Traffic shaping is used typically in confining the rate and limit of one stream in the output-network, so that this kind of message can be sent out steadily. Stream shaping is usually carried out by buffer and token bucket. When some groups' rate is too high, the message will be stored in buffer first, then it will be sent into the groups steadily.
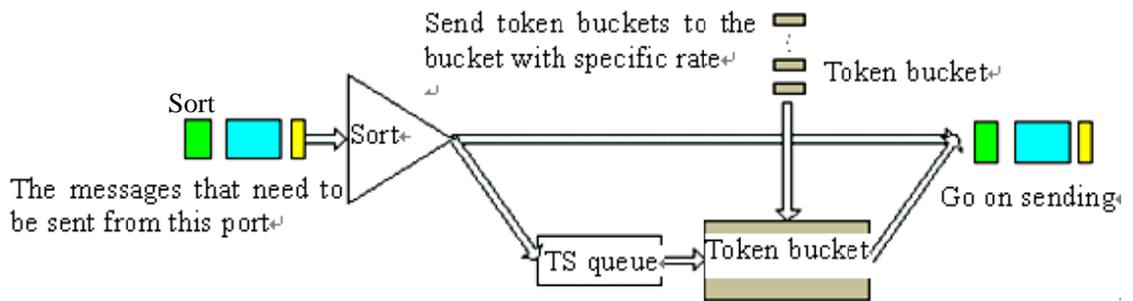
Figure 2 TS processing

TS can reshape given group stream or all the groups. When the groups come, it is classified first, and then continue transmission if there is no need for TS and token bucket. If TS is needed, the group will be compared with the token in token bucket. The token bucket put token in the bucket according to the rate that users set. If there is enough token for sending, the group will be sent, while the token number decreases according to the group length. When the token is the bucket is not enough for sending, the group will be stored in TS line. When there is group in the TS line, TS pick up one group and send it out periodically. Each sending will be compared with the token in the token bucket, until the token is not enough for the group in the line being sent out or all the groups in the line have been sent out.

For some purpose the bandwidth of the ports or VLAN needs to be confined. In this situation the bandwidth function needs to be configured that the port or VLAN bandwidth be confined in a range, the data that is over the bandwidth will be abandoned. By default, the ports and VLAN rate is auto negotiated, which need not to be confined.

The ingress port rate can be confined based on specified message and line priority. PIRL module uses speed confining resources to accomplish speed confining, aiming at the message type, message line privilege of the ingress port. Take MV6097 for example, this chip support 5 speed limitation resource every port, which is seized by global storm control, ports' message type and line privilege. Rate limitation is carried out by token bucket.

The model is as the following:
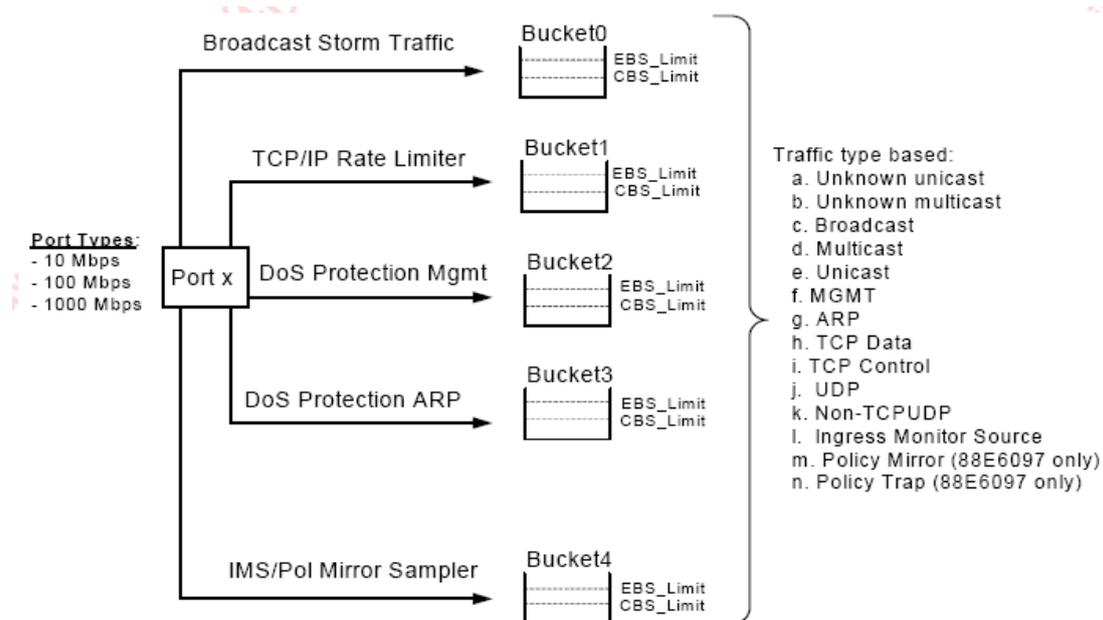
The speed limitation steps include: 64Kbps-1Mbps, the step is 64Kbps; 1Mbps-100Mbps, the step is 1Mbps; 100Mbps-1000Mbps, the step is 10Mbps.

Speed limitation aims at the following message type: ARP, TCP Data, TCP Ctrl, UDP, Non-TCPUDP, the line priority is 4. When the messages transmission speed exceeds the limit value, it can be abandoned or under traffic control.

5.2 Speed limitation and reshaping based on port function configuration

5.2.1. The default configuration

Function	Default value
The ingress port resource speed limitation message type, line priority calculation.	Or calculation relationship
When ingress port resource exceed the given speed limit	Drop drop
MAC no-speed limitation	Disabled
Port no-speed limitation function based on smac, dmac	Disabled

5.2.2. Port speed limitation and reshaping function

1. configure the ingress port bandwidth and burst:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rate-limit port-list** {**all** | *port-list*} **ingress** *rate* [*burst*]	Set the physical port bandwidth limit
		port-list physical port, ranging from 1 to the maximum number, use ',' and '-' for multi-port input:
		rate means the bandwidth, the unit is kbps, from 1 to 1048576.
		burst the burst，unit Kbps，can be set from 1 to 512. The actual value may be different from the value setting；
		ingress the ingress direction
3	**exit**	Quit global configuration mode and enter EXEC privileged mode
4	**show rate-limit port-list** [*port-list*]	Show port bandwidth limitation. *port-list* is accord with the meaning above.

What's special, the specified message and queue priority speed limitation can be set.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rate-limit port-list** *portlist* **ingress** *<1-1000000>* **queue-priority** {*1-4*}	Configure the port number, speed limitation value and message queue priority;
		Portlist is the physical port, the range is 1 to the maximum number, use ',' and '-' to carry out multi-port input;
		1-1000000 is the ingress port bandwidth, the unit is kbps;
		1-4 means queue priority.
3	**rate-limit port-list** *portlist* **ingress** *<1-1000000>*	Configure the speed configuration port and value;
		Portlist means the physical port, the range is 1 to max no.; use ',' and '-' to carry out multi-port input.
		1-1000000: ingress port bandwidth, the unit is kbps;
4	**rate-limit port-list** *portlist* **ingress** *<1-1000000>* [**arp**] [**tcp-data**] [**tcp-ctrl**] [**udp**]	Configure the speed configuration port and value；
		Portlist means the physical port, the range is 1 to max no.;

Step	Command	Description
	[**non-udptcp**]	use ',' and '-' to carry out multi-port input.
		1-1000000: ingress port bandwidth, the unit is kbps;
		arp: arp messages
		tcp-data: tcp data; message;
		tcp-ctr:tcp control message;
		udp: udp message;
		non-udptcp: includes IGMP, ICMP, GRE, IGRP, cisco, L2TP message;
5	**rate-limit port-list** *portlist* **ingress** *<1-1000000>* **queue-priority** {*1-4*} {**and**/**or**} [**arp**] [**tcp-data**] [**tcp-ctrl**] [**udp**] [**non-udptcp**]	Configure the speed configuration port and value;
		Portlist means the physical port, the range is 1 to max no.; use ',' and '-' to carry out multi-port input.
		1-1000000: ingress port bandwidth, the unit is kbps;
		or: calculation type;
		and calculation type: the ingress message;
		arp: arp message;
		tcp-data: tcp-data message;
		tcp-ctr: tcp control message;
		udp: udp message;
		non-udptcp: includes IGMP, ICMP, GRE, IGRP, cisco, L2TP message;
6	**exit**	Return to EXEC privileged mode;
7	**show interface port** *port_id* **rate-limit**	Show PIRL configuration information
		port_id port ID

Notice: PIRL (Port Ingress Rate Limiting) module confines the ingress port value in the following range: mega port <64-100000>kbps, giga port <64-100000>kbps; when the mega port configuration value exceeds 100000kbps, it will be set as 100000kbps. If there is no specified speed limitation message or message queue priority, all the messages will be limited. The configuration value might be different from the actual value, which is decided by the chip.

In PIRL module, when the speed limited message transmission speed exceeds the speed limitation, use **drop** and sending pause frame to handle it.

The configuration step is show as following:

Step	Command	Description
1	**config**	Enter global configuration mode;
2	**interface port** *<1-MAX_PORT_NUM>*	Enter Ethernet physical port mode; MAX_PORT_NUM the maximum port number that the equipment support;
3	[**no**] **rate-limit flow-control**	Configure flow-control mode, by default it is drop mode ;
4	**exit**	Return to EXEC privileged mode
5	**show interface port** *port_id* **rate-limit**	Show PIRL configuration information;

In PIRL mode, the specified MAC speed no-limitation is available only to the messages that has already entered the switch; if it fits the static MAC configuration, then there will be no such message speed limitation.

The configuration step is show as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mac-address-table static unicast** *HHHH.HHHH.HHHH* **vlan** *vlan_id* **port** *port-number* **none-rate-limit**	Configure the static MAC no-speed limitation function; *HHHH.HHHH.HHHH* static MAC address; Vlan id: VLAN ID, the range is 1~4094; *port-number* port number, the range is from 1to the maximum port number;
3	**exit**	Return to EXEC privileged mode
4	**show mac-address-table static**	Show MAC strategy configuration.

Open/close no-speed limit function based on **smac, dmac**, the configuration step is show below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port**<*1-MAX_PORT_NUM* >	Enter Ethernet physical port mode; *1-MAX_PORT_NUM* the port range that the equipment supports
3	**[no] rate-limit** {**smac**/**dmac**} **none-rate-limit**	Configure the no-speed limit function based on **smac,damc**;
4	**exit**	Return to global configuration mode
5	**show interface port** *port_id* **rate-limit**	Show PIRL configuration information; *Port id* port ID

2. Configure the ingress port bandwidth and burst:

Step	Command	Description
1	**config**	Enter global configuration mode
2		Configure the rate limiting.
	rate-limit port-list {**all**	*port-list*} **egress** *rate* [*burst*]	*port-list* physical port number, range is 1-26, use "," and "-" for multiple ports' rate limiting. *rate* stands for the maximum bandwidth allowed to be transmitted, unit is kbps, range is 1-1048576. (The actual value may be a little bit different from the configured value because it can only be the exponential of 2). *burst*: the configured bandwidth. Unit is KBps, the

		available value is 1-512. *The real value can be different with the configured value.*
		egress: the out traffic
3	**exit**	Exit from global configuration mode and enter privileged EXEC mode.
4	**show rate-limit port-list** [*port-list*]	Show the rate limiting of the port
		port-list physical port number, range is 1-26,use "," and "-" for multiple ports configuration.

To delete port speed limitation, use global configuration command **norate-limit port-list {all/***port-list***} {both | ingress | egress}**

5.2.3. Monitoring and maintaining

Use **show** to look over the switch's configuration and states of port speed limitation and PIRL function for the convenience of monitoring and maintaining. The relative command is show below:

Command	Description
show interface port *port_id* **rate-limit**	Show PIRL configuration
show mac-address-table static	Show MAC strategy configuration
show rate-limit port-list [*port-list*]	Show the port bandwidth limitation
	port-list strands for physical port number, range is 1-26, use ',' and '-' for multi-port ingress

5.2.4. Typical configuration example

➢ Aim

Configure the uplink bandwidth of the sw1's port 1 as 1000kbps, burst 64kbps, port 2 fits message **arp** and speed limit at message priority level 1-2, the speed limit value is 1000Kbps, open port 2 traffic control mode, so that the switch could manage the network traffic.

➢ Network structure:
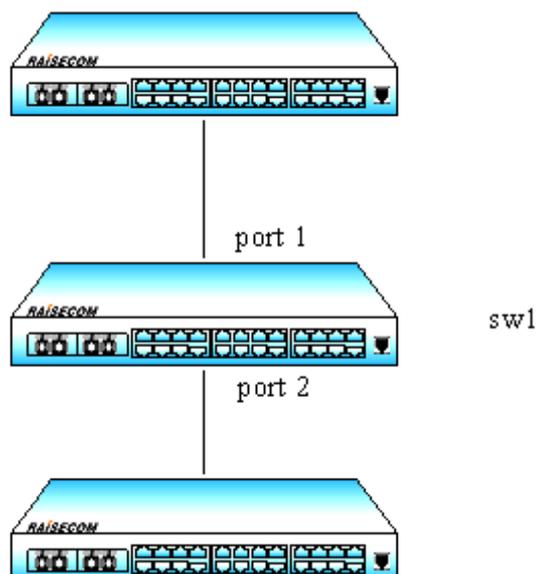
Figure 4 network structure

> Configuration step:

Step 1:

Raisecom#**config**

Raisecom(config)# **rate-limit port-list** *1* **ingress** *1000 64*

Set successfully

Actual ingress rate of FE port: 1000

Actual ingress burst of FE port: 64

Raisecom(config)#exit

Raisecom# show rate-limit port-list 1

I-Rate: Ingress Rate

I-Burst: Ingress Burst

E-Rate: Egress Rate

E-Burst: Egress Burst

Port	I-Rate(Kbps)	I-Burst(KBps)	E-Rate(Kbps)	E-Burst(KBps)
1	*1000*	*64*	*0*	*0*

Step 2:

Raisecom(config)# **rate-limit port-list** *2* **ingress** *100* **queue-priority** *1-2* **and arp**

Set successfully

Raisecom(config)#**interface port** *2*

Raisecom(config-port)# **rate-limit flow-control**

Set successfully

Raisecom#**show interface port** *2* **rate-limit**

port: 2

flow-control: Enable

smac-none-limit-rate: Disable

dmac-none-limit-rate: Disable

session	CIR(kbps)	BA(kBps)	rate-limit-operation	queue-priority	traffic-type
1	*100*	*128*	*and*	*1 2*	*arp*

5.3 Speed limitation and reshaping function based on VLAN configuration

5.3.1. The default configuration

By default, there is no bandwidth limit based on VLAN.

5.3.2. Speed limitation and reshaping function based on VLAN configuration

1. Configure speed limitation based on VLAN:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rate-limit vlan** *<1-4094> rate burst*	Set the traffic limitation based on VLAN. *<1-4094>*:VLANID; *Rate* strands for the bandwidth limitation based on VLAN, the unit is kbps, range is 1-1048576. The actual value may be different from the configured one. *burst* configured burst, the unit is Kbps,
3	**exit**	Exit from global configuration and enter EXEC privileged mode
4	**show rate-limit vlan**	Show the port speed limitation

2. configure the bandwidth and burst based on QinQ VLAN

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rate-limit double-tagging-vlan outer** {*<1-4094>*|**any**} **inner** {*<1-4094>*|**any**} *rate burst*	Configure the bandwidth limit based on QinQ VLAN; **outer** *{<1-4094>|any}* outer layer VLAN, *any* strands for any outer layer VLAN; **inner** *{<1-4094>|any}* lining VLAN, *any* strands for any outer layer VLAN; *rate* strands for the configured bandwidth value, the unit is kbps, range is 1-1048576,the actual value may be different from the configured value. *burst* the configured burst, the unit is kbps, the value can be set from 1 to 512. The actual value may be different from the configured value.
3	**exit**	Exit from global configuration mode and enter EXEC privileged mode.
4	**show rate-limit vlan**	Show the port bandwidth limitation.

Notice: The outer layer VLAN can not be un-assigned at the same time.

5.3.3. Monitoring and maintaining

Using **show,** the switch's VLAN speed limit configuration and state can be shown for the convenience of

monitoring and maintaining. The related command is shown below:

Command	Description
show rate-limit vlan	Show the port bandwidth limitation.

5.3.4. Typical configuration example

  ➢ Aim

Set the switch's VLAN 5 bandwidth as 2048kbps, the burst is 128kbps;

Set the outer layer VLAN as 6, lining VLAN as 10, the bandwidth 1024kbps, the burst 64kbps, to accomplish VLAN management.

  ➢ Configuration step:

Step 1:

Raisecom#**config**

Raisecom(config)# **rate-limit vlan** *5 2048 128*

  Set successfully

  Actual rate: 2048

  Actual burs: 128

Step 2:

Raisecom(config)# **rate-limit double-tagging-vlan outer** *6* **inner** *10 1024 64*

  Set successfully

  Actual rate: 1024

  Actual burs: 64

Raisecom(config)#**exit**

Raisecom# **show rate-limit vlan**

  CVLAN: Customer VLAN(inner VLAN)

  SPVLAN:Service provider VLAN(outer VLAN)

Type	*CVLAN*	*SPVLAN*	*Rate(Kbps)*	*Burst(KBps)*
single	*5*	*--*	*2048*	*128*
double	*10*	*6*	*1024*	*64*

Chapter 6 MAC Address Table

6.1 MAC transmission table management introduction

6.1.1 MAC address transmission table

The Ethernet switch's main function is to transmit message in data link layer, that is to transmit messages to the corresponding port according to the destination MAC address. MAC address transmission table is a two-ply table that contains MAC address and transmission port matchup, which is the base of the Ethernet switch transmitting two-ply messages.

MAC address transmission table contains the following information:

➢ The destination MAC address;
➢ The VLAN ID belongs to the port;
➢ The transmission egress port number of the local equipment;

When the Ethernet switch is transmitting messages, according to the MAC address table information, the following way is available:

➢ Unicast: when there is table item that fits the message destination MAC address in the MAC address transmission table, the switch will transmit it directly from the transmission egress port of the table item;
➢ Broadcast: when the messages that the switch received from the destination address are all F, or when there is no table item that is accord with the message destination MAC address in the MAC address transmission table, the switch will use broadcast and transmit the message to all the ports except the receive ports.

6.1.2 MAC address learning

The table item in MAC address table can be upgraded and maintained through the following two ways:

➢ Manual configuration
➢ MAC address learning

Usually, most MAC address is created and maintained by the MAC address function. The Ethernet switch learning MAC address process is shown below:
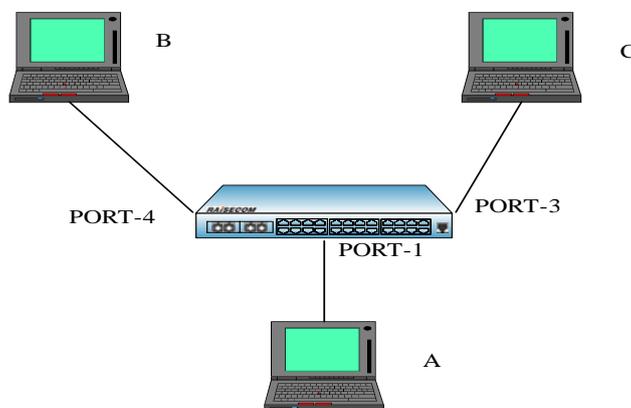
Fig 1 Mac address learning

When User A need to communicate with User B in the same VLAN1, the message need to be sent to the

switch's port 1, while the switch record the message's source MAC address, or User A's address 'MAC-A', to its own MAC address transmission table.

When the learning process is done, the switch will transmit the message. Because there is no MAC address and port table item, the switch will transmit the message to all the port except port 1 to confirm that User B could receive the message;

Because the switch use broadcast to transmit the message, both User B and User C will receive the message, while User C is not the destination equipment, so he will not process it. Normally, User B will respond User A by sending messages. When the response message is sent to port 4, the switch will use the same MAC address learning way and save User B's address and port corresponding relationship in the MAC address transmission table.

By this time there will be two table item in the switch's transmission table. When transmitting response message, because there has already been the table item that the destination is 'MAC-A' in the MAC address transmission table, the switch will no longer use broadcast, but send the message directly to User A through port 1 to accomplish the message interaction.

The way above is independent MAC address learning, or IVL, while there is another way for learning MAC address, that is share-VLAN MAC address learning, or SVL. By default, the switch use IVL mode, and SVL mode needs to be set in some cases.

6.1.3 MAC address table management

1. MAC address transmission table aging mechanism:

The switch MAC address transmission table has limitation in capacity, so it use aging mechanism to refresh the MAC address transmission table to make full use of the address transmission table resource. That is, the system open the aging timer when it is creating one table item dynamically, and if there is no more messages received from the MAC address of the table item in the aging time, the switch will delete the MAC address table item.

Notice:

➢ When 'destination MAC address refresh' function is enabled, if the switch transmits a message which the destination is one MAC address in the aging time, the MAC table item will be refreshed, and restart aging;
➢ MAC address aging mechanism is valid only to dynamic MAC address table item.

2. MAC address table sorts and features:

➢ Static MAC address table item: or 'permanent address', it is added or deleted by user, without aging. For a network in which the equipments change rarely, manually adding static address table item can reduce the network broadcast traffic.
➢ Dynamic MAC address table item: it stands for the MAC address table item that ages according to the aging time that user set. The switch could add dynamic MAC address table item through MAC address learning mechanism or user handwork.

6.2 MAC address transmission table management configuration

6.2.1 The default MAC address transmission table configuration

Function	Default value

MAC address aging time	300s
MAC address learning feature	Enable
Static MAC address privilege	-1（N/A in command lines）
Static MAC address MAC strategy	Transmit normally
Static MAC address no-speed-limit	enable

6.2.2 Static MAC address configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mac-address-table static unicast** *HHHH.HHHH.HHHH* **vlan** *vlan id* **port** *port-number*	Set the static MAC address. *HHHH.HHHH.HH*HH is the static MAC address which will be set; format is hex, dotted notation for every four characters. Vlan_id range is 1-4094. *port_number* is the physical port number.
3	**mac-address-table static multicast** *HHHH.HHHH.HHHH* **vlan** *vlan_id* **port** *port-list*	Set the static MAC address. *HHHH.HHHH.HHHH is the static MAC address which will be set; format is hex,* dotted notation for every four characters. Vlan_id range is 1-4094. *port_number* is the physical port number, range is 1-26, use ',' or '-' to input the port list.
4	**exit**	Exit global configuration mode and enter privileged EXEC mode
5	**show mac-address-table static** [**port** *port-number*	**vlan** *vlan_id*]	Show (port or VLAN) static address. *port_number* is physical port, range is 1-26. *vlan_id:* range is 1-4094.

Note: The switch MAC address, multicasting address, FFFF.FFFF.FFFF and 0000.0000.0000 can not be configured as the static MAC address.

6.2.3 MAC address aging time configuration

The dynamic source MAC address that the switch has learned will age when it is not in use. The aging time can be changed, and the MAC address aging can be disabled. By default, the aging time is 300s.

Step	Command	Description
1	**config**	Enter global configuration mode

		Set the aging time of MAC address table.
2	**mac-address-table aging-time** {*0* | *time*}	0 stands for MAC address will not be aged
		time is the target MAC address aging time, unit is second, range is 3-765, and default value is 300.
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show mac aging-time**	Show MAC address aging time

To Restore the default value, use the command **no: no mac-address-table aging-time**.

6.2.4 MAC address learning enable/disable

Sometimes disable/enable a certain physical port learning MAC address is needed, which can be achieved by configuring the switch of MAC address learning ability. By default, every physical port can be allowed to learn MAC address.

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**mac-address-table learning** {**enable** | **disable**} **port-list** {**all** | {1-26}}	Enable or disable the MAC address learning function of physical port.
		enable enable MAC address learning function.
		disable disable MAC address learning function.
		MAX_PORT_NUM the maximum port number that the equipment support
3	**exit**	Exit from global configuration mode to privileged EXEC mode.
4	**show interface port** [*port-number*]	Show port status.
		port_number physical port,range is 1-26.

6.2.5 Clear MAC address table

Clear layer-2 MAC address table entries of the switch, includes static and dynamic MAC address. The command can be used in global configuration mode.

Step	Command	Description
1	**clear mac-address-table** {*all*/*dynamic*/*static*}	**all:** delete all the 2 MAC addresses in the MAC address table
		dynamic: delete dynamic MAC addresses in the MAC address table
		static: delete static MAC addresses in the MAC address table

6.2.6 Configure static MAC address privilege

The static MAC address privilege value range is 0~7, the default value is -1, and the command line shows N/A when it is -1.

The configuration step is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mac-address-table static unicast** *HHHH.HHHH.HHHH* **vlan** *vlan_id* **port** *port-number* **[priority <0-7>]**	Set static MAC address *HHHH.HHHH.HHHH* is the static MAC address which will be set; format is hex, dotted notation for every four characters. *vlan_id* VLAN ID, range is 1~4094. *port_number* physical port number configure the privilege value, range is 0~7
3	**exit**	Quit global configuration mode and enter privileged EXEC mode.
4	**show mac-address-table static** [**port** *port-number* | **vlan** *vlan_id*]	Show (port or VLAN) static address *port_number* physical port number *vlan_id* VLAN ID, range is 1~4094.

To restore static MAC address default privilege (-1), use **no: no mac-address-table static unicast** HHHH.HHHH.HHHH **vlan** vlan id **priority.**

6.2.7 enable/disable static MAC strategy

Static MAC address MAC strategy includes normal transmission (default), mirror and drop, all of which are based on port. This command enable global switches.

The step is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mac-address-table static unicast** *HHHH.HHHH.HHHH* **vlan** *vlan_id* **port** *port-number* **[mac-policy]**	Set static MAC configuration *HHHH.HHHH.HHHH* static MAC address which is to be set, format is hex, dotted notation for every four characters. *vlan_id* VLAN ID, range is 1~4094. *port_number* physical port number **mac-policy** enable MAC strategy.
3	**exit**	Quit global configuration mode and enter privileged EXEC mode.
4	**show mac-address-table static** [**port** *port-number* | **vlan** *vlan_id*]	Show (port or VLAN) static address *port_number* physical port number *vlan_id* VLAN ID, range is 1~4094.

To close static MAC address MAC strategy default configuration, use **no: no mac-addresss-table static unicast** HHHH.HHHH.HHHH **vlan** vlan id **mac-policy.**

6.2.8 Enable/disable static MAC address non-rate-limit

Static MAC address can be set non-rat-limit. To the given MAC address, with non-speed-limit configuration, the messages into the MAC address have no speed limit.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mac-address-table static unicast** *HHHH.HHHH.HHHH* **vlan** *vlan_id* **port** *port-number* [**non-rate-limit**]	Set static MAC configuration *HHHH.HHHH.HHHH* static MAC address which is to be set, format is hex, dotted notation for every four characters. *vlan_id* VLAN ID, range is 1~4094. *port_number* physical port number **non-rate-limit** non-rate-limit feature
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show mac-address-table static** [**port** *port-number* | **vlan** *vlan_id*]	Show (port or VLAN) static address *port_number* physical port number *vlan_id* VLAN ID, range is 1~4094.

To close static MAC address non-rate-limit, use **no: no mac-address-table static unicast** HHHH.HHHH.HHHH.HHHH **vlan** vlan_id **non-rate-limit**

6.2.9 Monitoring and maintaining

Use **show** to look over MAC address transmission table configuration:

Command	Description
show mac aging-time	Show MAC address aging time
show mac-address-table l2-address port *port-number*	Show the switch port MAC address *Port_number* physical port, range is 1~26
show mac-address-table l2-address vlan *vlan_id*	Show the switch port MAC address *vlan_id* VLAN ID, range is 1~4094
show mac-address-table l2-address count port *port-number*	Show the switch port MAC address number **Count** stands for the MAC address number related to the statistics *port_number* physical port number, range is 1~26.
show mac-address-table l2-address count vlan *vlan_id*	Show the switch VLAN MAC address **Count** stands for the MAC address number related to the statistics *vlan_id* VLAN ID, range is 1~4094
show mac-address-table static	Show the switch static MAC address configuration information
show mac-policy portlist *portlist*	Show the MAC strategy of each port

Especially, the command for searching the information of a certain MAC address in the switch.

Command	Description
search mac-address *HHHH.HHHH.HHHH*	Search for MAC address *HHHH.HHHH.HHHH* static MAC address which is to be set, format is hex, dotted notation for every four characters.

6.2.10 Typical configuration example

➢ Destination:

Enable all the ports' MAC address learning function of the switch;

Configure a static unicast MAC address 1234.1234.1234 in port 2, VLAN 10;

Set the aging time 100s, observe the switch MAC address learning and aging situation.

➢ Network figure
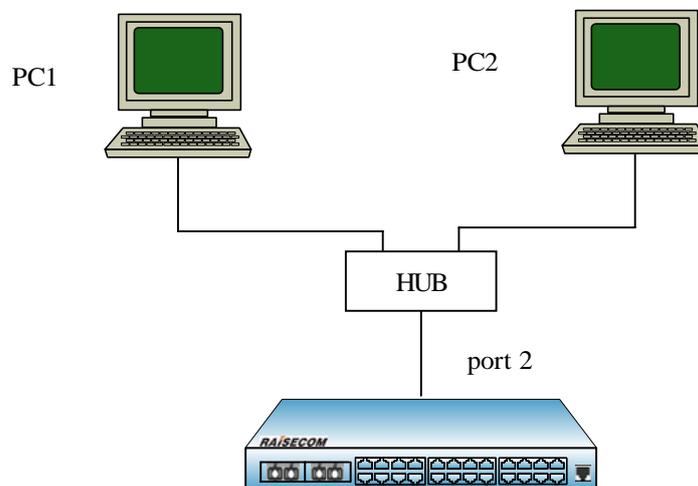
Fig 2 network

➢ Configuration step

Step 1:

Enable all the ports' MAC address learning function

Raisecom(config)#**mac-address-table learning** *enable* **port-list** *all*

Step 2:

Set static unicast MAC address 1234.1234.1234.1234 in port 2, VLAN 10

Raisecom(config)#**interface port** *2*

Raisecom(config-port)#**switchport access vlan** *10*

Raisecom(config)#**mac-address-table static unicast** *1234.1234.1234* **vlan** *10* **port** *2*

Step 3:

Set the aging time as 100s

Raisecom(config)#**mac-address-table aging-time** *100*

We can notice that the switch can learn 2 dynamic MAC address through port 2, which age 100s later, then restart learning, while static MAC address will no age.

6.3 MAC address number limit

With MAC address learning function, the Ethernet switch can get the MAC address within the same network segment. To the message that is sent to the MAC addresses, the Ethernet switch use hardware for transmission through looking for MAC address transmission table to raise the transmission efficiency. If the MAC address transmission table is much too large, the time of looking for the corresponding transmission table item may be prolonged, and the switch transmission function will drop. By configuring the maximum MAC address number that the Ethernet port can learn, the administrator is able to control the MAC address transmission table item number that the Ethernet switch maintains. When the MAC address number that the port has learned rises to the maximum value that user set, the port will no longer learn MAC address.

6.3.1 Configure the default MAC address number limit

By default, the MAC address learning number has no upper limit.

6.3.2 Configure the MAC address number

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface { port | line | client}** *<1-MAX_PORT_NUM >*	Enter Ethernet physical port mode
3	**mac-address-table threshold <** *PORT_MAC_MIN_THRESHOLD_STR - PORT_MAC_MAX_THRESHOLD_STR>*	Configure the MAC address learning upper limit *PORT_MAC_MIN_THRESHOLD_ STR* value upper limit *PORT_MAC_MAX_THRESHOLD_ STR* value lower limit
4	**exit**	Quit global configuration mode and enter privileged EXEC mode
5	**show interface mac-address-table threshold**	Show interface mac address table threshold value

6.3.3 Monitoring and maintaining

Command	Description
show interface mac-address-table threshold	Show interface MAC address table threshold value
Show mac-addres l2	Show interface MAC address number that has been learned

6.3.4 Typical configuration example

➢ Destination

Configure the MAC address learning threshold of the switch port as 1, and the switch won't learn the dynamic MAC address that extend the threshold value.

➢ Network

PC1   PC2

HUB
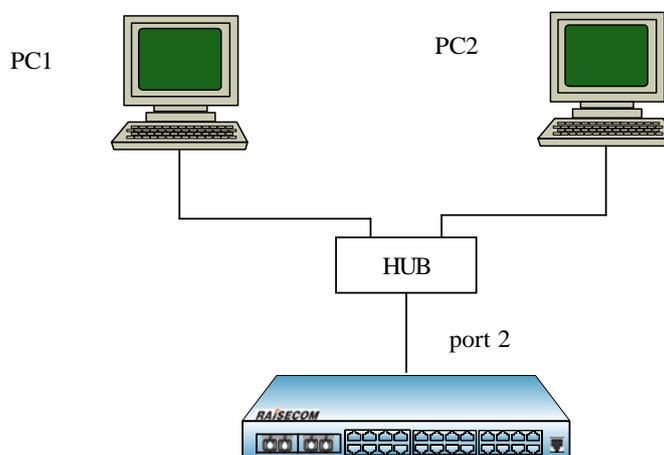
port 2

Fig 3   network

➢ Configuration step

Step 1:

The upper limit of port 2 learning MAC address is 100

Raisecom(config-port)#**mac-address-table threshold** *1*

Step 2:

Show interface MAC address learning number:

Raisecom# **show mac-address-table** *l2*-**address count port** *1*

Port 2 shows only 1 dynamic MAC is learned.

Step 3:

Cancel the MAC learning confirmation of port 2

Raisecom(config-port)#**no mac-address-table threshold**

Show interface MAC address learning number:

Raisecom# **show mac-address-table** l2-**address count port** *1*

Port 2 shows there are 2 dynamic MAC that has been learned.

6.4 Shared VLAN learning function

6.4.1 The default SVL configuration

Function	Default value

SVL feature	Disabled
Interface SVL default VLAN list	Empty
SVL default VLAN	VLAN 1

6.4.2 SVL configuration

The step is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**svl** {*enable* / *disable*}	Enable/disable SVL mode
3	**interface port** *<1-MAX_PORT_NUM>*	Enter port configuration mode *1-MAX_PORT_NUM* the port number that the equipment supports
4	**switchport svl vlanlist** {*1-4094*}	Optical Set the shared VLAN list of the port
5	**exit**	Enter global configuration mode
6	**svl default vlan** *<1-4094>*	Set SVL default VLAN *1-4094*:VLAN ID
7	**exit**	Quit global configuration mode and enter privileged EXEC mode
8	**show svl**	Show SVL state
9	**show switchport** [*<1-MAX_PORT_NUM>*] **svl vlanlist**	Show interface shared VLAN list *1-MAX_PORT_NUM* the port number that the equipment supports
10	**show svl default vlan**	Show SVL default VLAN

Notice: When some port is not configured the SVL VLAN list, the MAC will be shared to SVL default VLAN.

6.4.3 Monitoring and maintaining

Command	Description
Show svl	Show SVL state
show switchport [*<1-MAX_PORT_NUM>*] **svl vlanlist**	Show interface shared VLAN list *1-MAX_PORT_NUM* the port number that the equipment supports
Show svl default vlan	Show SVL default VLAN

6.4.4 Typical configuration example

➢ Destination

Enable the switch SVL function, and share the MAC address learned in port 1 between VLAN 1-4;

➢ Configuration step

Step 1:

Enable SVL mode

Raisecom # **config**

Raisecom (config)# **svl** *enable*

Raisecom (config)# **exit**

Raisecom # **show svl**

   SVL: Enable

   Step 2:

   Set port 1 shared VLAN 1-4

Raisecom#**config**

Raisecom(config)#**interface port** *1*

Raisecom(config-port)# **switchport svl vlanlist** *1-4*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom# **show switchport** *1* **svl vlanlist**

   Port   SVL   VLAN list

Chapter 7 Interface

7.1 Physical ports features

For a switch, whatever the equipment is, physical interface is necessary for connection. And physical ports have many features, any message that is entering or leaving the switch needs physical ports to transmit, so the function of physical port is relatively more difficult, which is also very important; to some of the function manual configuration is available, like port rate, duplex mode, negotiation mode, crossover cable automatic recognition and system maximum transmission unit, all of which are the features of the physical ports. To the certain use, the corresponding setting is needed for the physical port to receive or transmit messages.

7.2 The default configuration for physical ports

By default, the physical port commands is shown below:

Command	Default value
Rate configuration	The rate of electronic port and 100M optical port is auto negotiated, 100M iptical port rate is 100M by default
Duplex mode configuration	The rate of electronic port and 100M optical port is auto negotiated, 100M optical port in duplex is full duplex
Rate control configuration	Physical port rate control function is off
Crossover Ethernet cable auto-recognition and straight Ethernet cable function	Normal mode
Port maximum transmission unit	1522 byte
Interface on/off configuration	on

7.3 Rate and duplex mode configuration

Gigabit port is always working in 1000Mbps and full duplex mode. When auto negotiation function is enabled, the duplex mode (speed) will be set according to the result auto negotiation. In default situation, auto negotiation is enabled for all the electronic ports and 1000M optical port, only the default value of 100M optical port is 100M/FD.

Rate and duplex mode configuration step is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**interface port** *port-number* **interface range** *port-list*	Enter Ethernet physical interface configuration mode or physical interface range configuration mode. *port_number* is the physical interface, range is 1-26.

		*port-list r*ange is 1-26, use "," and "-"for multiple interfaces configuration.
3	**speed** *{auto|10|100|1000}* **duplex** *{full|half}*	Set the speed and duplex mode of the port. *auto*: represents that both the speed and duplex are set according to the result of auto negotiation. *10*: represents that the speed is set to 10Mbps. *100*: represents that the speed is set to 100Mbps. *1000*: represents that the speed is set to 1000Mbps. *full*: set the duplex mode to full duplex. *half*: set the duplex mode to half duplex.
4	**exit**	Exit from Ethernet physical interface configuration mode to global configuration mode.
5	**exit**	Exit from global configuration mode to privileged EXEC mode
6	**show interface port** *port-number*	Show the status for the port. *port_number* physical port, range is 1-26.

Note:

➢ Using the Ethernet interface configuration mode **speed auto**, the rate and duplex mode will be restored to auto negotiation by default.

➢ Different ports fit different rate and duplex mode. 100M electronic ports can not be set to 1000M, 100M optical port can be set to 100M/FD only, 1000M optical port can be only configured 1000M/FD/auto, while extended card port can not be configured rate and duplex mode when the extended card does not exist.

Example 1: set the speed of port 15 to 10Mbps, duplex mode is full duplex.

Raisecom#**config**

ISCOM2826(config)#**interface port** *15*

ISCOM2826(config-port)#**speed** *10*

ISCOM2826(config-port)# **duplex** *full*

ISCOM2826(config-port)#**exit**

ISCOM2826(config)#**exit**

Raisecom#**show interface port** *15*

R: Receive Direction

S: Send Direction

Port	Admin	Operate	Speed/Duplex	Flowcontrol(R/S)	Mac-learning
15	enable	down	10/full	off/off	enable

Example 2: set the rate of 100M optical port to 10Mbps, duplex mode is half-duplex.

Raisecom#**config**

Raisecom(config)#**interface port** *1*

Raisecom(config-port)#**speed** *10*

 Port 1 only supports 100M/FD!/ port1 support only100M/FD!

Raisecom(config-port)# **duplex** *half*

 Port 1 only supports 100M/FD!/ port1 support only 100M/FD!

Example 3: set 1000M optical port P2 to 100Mbps, duplex mode is half-duplex

Raisecom#**config**

Raisecom(config)#**interface port** *2*

Raisecom(config-port)#**speed** *100*

 Port 2 only supports 1000M/FD or auto-negotiation!/ port 2 support only 100M/FD or auto negotiation.

Raisecom(config-port)# **duplex** *half*

 Port 2 only supports 1000M/FD or auto-negotiation!/ port 2 support only 100M/FD or auto negotiation.

Example 4: set 100M electronic port P3 to 1000Mbps

Raisecom#**config**

Raisecom(config)#**interface port** *3*

Raisecom(config-port)#**speed** *1000*

 Port 3 does not support 1000M!/port 3 do not support 1000M!

Example 5: set extended card P25 to 1000Mbps

Raisecom#**config**

Raisecom(config)#**interface port** *25*

Raisecom(config-port)#**speed** *1000*

 Port 25 is unavailable!/ port 25 does not exist.

7.4 Configure IEEE 802.3X flow control function

The flow control function of Raisecom series switches is set on both RX and TX direction, that is to say, you can set the interface's ability to receive and send pause frame to on/off separately. By default, flow control function is disabled on both directions. For extended card port, if there is no corresponding extended card inserted, the flow control commands fail.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** *port-number* **interface range** *port-list*	Enter Ethernet physical interface configuration mode or range configuration mode. *port_number* physical ports, range is 1-26.

		port-list, range is 1-26,use "," and "-" for multiple ports.
3	**flowcontrol** *{receive|send}{on|off}*	Enable/disable the flow control function on RX and TX direction.
		Send represents the traffic control function at TX direction.
		receive: represents the traffic control function at RX direction.
		on: enabe the flow control function of the port.
		off: disable the flow control function of the port.
4	**exit**	Exit from the physical interface configuration mode and enter global configuration mode.
5	**exit**	Exit from global configuration mode and enter privileged EXEC mode.
6	**show interface port** *port-number*	Show the traffic control of the port.
		port_number physical port number, range is 1-26.

Example 1: Set the flow control for port 10.

Raisecom#**config**

ISCOM2826(config)# **interface port** *10*

ISCOM2826(config-port)#**flowcontrol receive** *on*

ISCOM2826(config-port)#**exit**

ISCOM2826(config)#**exit**

Raisecom#**show interface port** *10*

R: RX Direction

S: tx Direction

Port	*Admin*	*Operate*	*Speed/Duplex*	*Flowcontrol(R/S)*	*Mac-learning*
10	*enable*	*down*	*auto*	*on/off*	*enable*

Example 2: set the extended card P25 flow control function on.

Raisecom#**config**

Raisecom(config)#**interface port** *25*

Raisecom(config-port)# **flowcontrol** *on*

Port 25 is unavailable! /port 25 does not exist!

For some equipment, the flow control situation of the ports' receiving direction and sending direction is configured respectively. By default all the ports' flow control is off.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** *port-number*	Enter physical port mode or interface range

	interface range *port-list*	configuration mode.
		port_number physical port number, range is 1-26
		port-list port list, range is 1-26, use ',' and '-' for multiple setting.
3	**flowcontrol** *{receive/send}{on/off}*	Configure physical port flow control function on/off
		send strands for the flow control function of the sending direction;
		receive strands for flow control function of the receiving direction;
		on enable interface flow control function;
		off disable interface flow control function
4	**exit**	Quit physical port configuration mode and enter global configuration mode
5	**exit**	Quit global configuration mode and enter privileged EXEC mode
6	**show interface port** *port-number*	Show interface flow control state; *port_number* physical port number.

For example: set port 10 flow control function on receiving direction to on.

Raisecom#**config**

Raisecom(config)# **interface port** *10*

Raisecom(config-port)#**flowcontrol receive** *on*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show interface port** *10*

R: Receive Direction

S: Send Direction

Port	*Admin*	*Operate*	*Speed/Duplex*	*Flowcontrol(R/S)*	*Mac-learning*
10	*enable*	*down*	*auto*	*on/off*	*enable*

For some equipments, the flow control situation of the ports' receiving direction and sending direction is configured respectively, but the result take effect at the same time, that is to say, changing the flow control setting of any direction will effect the flow control configuration of both side, on or off at the same time. By default all the ports' flow control is off.

Step	**Command**	**Description**
1	**config**	Enter global configuration mode
2	**interface port** *port-number* **interface range** *port-list*	Enter physical port mode or interface range configuration mode; *port_number* physical interface number; *port-list* port list, use ',' and '-' for multiple setting.

		Configure physical port flow control function on/off
		Send strands for the flow control function of the sending direction;
3	**flowcontrol** *{receive|send} {on|off}*	Receive strands for flow control function of the receiving direction;
		on enable flow control function
		Off disable port flow control function
4	**exit**	Quit physical port configuration mode and enter global configuration mode;
5	**exit**	Quit global configuration mode and enter privileged EXEC mode;
6	**show interface port** *port-number*	Show the port flow control state
		port_number physical port number.

For example: enable port 10 flow control function

Raisecom#**config**

Raisecom(config)# **interface port** *10*

Raisecom(config-port)#**flowcontrol receive on**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show interface port** *10*

R: Receive Direction

S: Send Direction

Port	*Admin*	*Operate*	*Speed/Duplex*	*Flowcontrol(R/S)*	*Mac-learning*
10	*enable*	*down*	*auto*	*on/on*	*enable*

7.5 Auto-MDIX function configuration

The function of Auto-MDIX is to auto-recognize crossover Ethernet cable and straight Ethernet cable. The configuration step is show below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** *port-number* **interface range** *port-list*	Enter physical port mode or interface range configuration mode; *port_number* physical interface number; *port-list* port list, use ',' and '-' for multiple setting.
3	**mdi** *(auto |normal |across)*	Configure port MDI mode; auto linear ordering auto reserve mode normal normal mode

		across cross mode
4	**exit**	Quit physical port configuration mode and enter global configuration mode
5	**exit**	Quit global configuration mode and enter privileged EXEC mode
6	**show mdi** [*<1-MAX_PORT_STR>*]	Show port MDI state *<1-MAX_PORT_STR>*: physical port

For example: set port 8 Auto-MDIX function to auto mode.

Raisecom#**config**

Raisecom(config)# **interface port** *8*

Raisecom(config-port)#**mdi auto**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show mdi** *8*

> *Port 8 MDI mode :auto Current status :across*

7.6 Line detection function

Line detection function is to detect the Ethernet port connection line, by which user can look over the state of the physical lines. The line information acquired from line detection module includes:

Detect line state:

Normal- line connection is normal

Open- circuit open

Shorted- circuit shorted

Error

Detect error position

The line sends error position

The line receives error position

Step	Command	Description
1	**test cable-diagnostics port-list** (*all|portlist*)	Begin cable diagnoses. *all* all the physical ports *portlist* physical ports list
2	**show cable-diagnostics port-list** (*all|portlist*)	Show cable diagnoses information *all* all the physical ports *portlist* physical ports list

For example: run cable diagnoses and show the result.

Raisecom#**test cable-diagnostics port-list** *all*

Raisecom#**show cable-diagnostics port-list** *all*

Port	Attribute	Time	RX Stat	RX Len(m)	TX Stat	TX Len(m)
1	*Issued*	*01/01/2000 08:05:33*	*Open*	*1*	*Open*	*1*
2	*Issued*	*01/01/2000 08:05:33*	*Open*	*1*	*Open*	*1*
3	*Issued*	*01/01/2000 08:05:34*	*Open*	*1*	*Open*	*1*
4	*Issued*	*01/01/2000 08:05:34*	*Open*	*1*	*Open*	*1*
5	*Issued*	*01/01/2000 08:05:34*	*Open*	*1*	*Open*	*1*
6	*Issued*	*01/01/2000 08:05:34*	*Open*	*1*	*Open*	*1*
7	*Issued*	*01/01/2000 08:05:34*	*Open*	*1*	*Open*	*1*
8	*Issued*	*01/01/2000 08:05:34*	*Normal*	*0*	*Normal*	*0*
9	*Issued*	*01/01/2000 08:05:34*	*Open*	*1*	*Open*	*1*
10	*Issued*	*01/01/2000 08:05:34*	*Open*	*1*	*Open*	*1*
......						
24	*Issued*	*01/01/2000 08:05:34*	*Open*	*1*	*Open*	*1*
25	*Not Support*	*N/A*	*N/A*	*0*	*N/A*	*0*
26	*Not Support*	*N/A*	*N/A*	*0*	*N/A*	*0*

Explain: States:

➢ Normal- line connection normal
➢ Open- circuit open
➢ Shorted- circuit shorted
➢ Error
➢ N/A- invalid

Attribution:

➢ Issued- test over
➢ Not Issued- no test
➢ Testing- testing
➢ Not Support- not support

7.7 Maximum transmission unit configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**system mtu** *<1500-8000>* **no system mtu**	Set maximum transmission unit; <1500-8000> system maximum transmission unit range; Delete maximum transmission unit configuration
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show system mtu**	Show system maximum transmission unit

	configuration

For example: set system maximum transmission unit to 5000.

Raisecom#**config**

Raisecom(config)# **systemc mtu** *5000*

Raisecom(config)#**exit**

Raisecom#**show system mtu**

System MTU size: 5000 bytes

7.8 Add description for interfaces

Description of the Physical port and IP port can be added.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** *port-number*	Enter physical layer port configuration mode or volume configuration mode *port_number* physical port number, range is 1-26
3	**[no]description** *WORD*	Add physical port or IP interface decription *WORD*——specify class-map decription. 255 character the most, can not be departed by space.
4	**exit**	Quit physical layer port configuration mode and enter global configuration mode.
5	**exit**	Quit global configuration mode and enter privileged EXEC mode.
6	**show interface port** [*<1-MAXPORT>*] **detail**	Show port information <1-MAXPORT> port number.

Example 1: add decription for physical port 20.

Raisecom#**config**

Raisecom(config)# **interface port** *20*

Raisecom(config-port)# **description** *this-is-a-class-map*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show interface port** *20* **detail**

7.9 Open and close physical layer port

Sometimes, for a certain intention, to close physical ports is needed, and configuring the ports' on/off is necessary. By default all the ports are on. To extended card port, physical port on/off commands are invalid when the card is not inserted.

Step	Command	Description

1	**config**	Enter global configuration
2	**interface port** *port-number* **interface range** *port-list*	Enter physical layer port configuration mode or volume configuration mode. *port_number* physical port number. *port-list* port list, use ',' and '-' to make multi-port input.
3	*{shutdown | no shutdown}*	Close or open physical port. shutdown stands for closing physical port. no shutdown stands for opening physical port.
4	**exit**	Quit physical layer interface configuration mode and enter global configuration mode
5	**exit**	Quit global configuration mode and enter privileged EXEC mode.
6	**show interface port** *port-number*	Show port state *port_number* physical port number.

Example 1: close port 20.

Raisecom#**config**

Raisecom(config)# **interface port** *20*

Raisecom(config-port)#**shut down**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show interface port** *20*

R: Receive Direction

S: Send Direction

Port	*Admin*	*Operate*	*Speed/Duplex*	*Flowcontrol(R/S)*	*Mac-learning*
20	*enable*	*down*	*auto*	*off/off*	*enable*

Example 2: close extended card port P25 (without extended card inserted)

Raisecom#**config**

Raisecom(config)#**interface port** 25

Raisecom(config-port)# **shut down**

Port 25 is unavailable!

7.10 Monitoring and maintaining

Use **show** to show port state.

Command	Description
show interface port *port-number*	Show port state *port_number* physical port number.
show interface port [<*1-MAXPORT*>] **detail**	Show port information. *<1-MAXPORT>* port number.

For example: show port 8 state.

Raisecom#**show interface port** *8*

R: Receive Direction

S: Send Direction

Port	Admin	Operate	Speed/Duplex	Flowcontrol(R/S)	Mac-learning
8	enable	down	auto	off/off	enable

Chapter 8 Storm Control

8.1 Storm control introduction

A packet storm occurs when a large number of broadcast, unicast, or DLF packets are received on a port. Forwarding these packets can cause the network to slow down or to time out. Storm control is configured for the switch as a whole but operates on a per-port basis. By default, storm control is enabled.

8.2 The default configuration for storm control function

By default, storm control is enabled for unicast DLF packets, broadcast packets and mulicast packets.

8.3 Storm control function configuration

8.3.1 Enable/disable storm control function

The configuration is to enable/disable storm control

Step	Command	Description
1	**config**	Global configuration mode
2	**storm-control** *{broadcast / multicast / dlf / all}* *{enable / disable}*	Enable/disable broadcast packet, multicast packet and DLF packet
		Broadcast DLF broadcast packet
		Multicast DLF multicast packet
		Dlf DLF packet
		All broadcast, multicast and DLF unicast packets.
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show storm-control**	Show storm control state

8.3.2 Storm control number

Configure storm control threshold, unit is kbps (kbit per second).

Step	Command	Description
1	**config**	Enter global configuration mode
2	**storm-control bps** *value*	Set storm control threshold. Value stands for the kbit number that is allowed to pass per second, range can be found on the command manual.
3	**exit**	Quit global configuration mode and enter

		privileged EXEC mode.
4	**show storm-control**	Show storm control state.

Configure storm control threshold, unit is pps (packet per second).

Step	Command	Description
1	**config**	Enter global configuration mode
2	**storm-control pps** *value*	Set storm control threshold. Value the storm packet number that is allowed to pass per second, range is 0-262143.
3	**exit**	Quit global configuration mode and enter privileged EXEC mode.
4	**show storm-control**	Show storm control state.

Set storm control threshold for broadcast, multicast and DLF packets, unit is %

Step	Command	Description
1	**config**	Enter global configuration mode
2	**torm-control ratio** *<1-100>* [*<0-512>*]	Set storm control threshold for broadcast, multicast and DLF packets, unit is % 1-100 the bandwidth proportion of the storm packet 0-512 burst value, unit is Kbps；
3	**exit**	Quit global configuration mode and enter privileged EXEC mode.
4	**show storm-control**	Show storm control state.

8.4 Monitoring and maintaining

Command	Description
show storm-control	Show storm control state

8.4 Typical configuration example

Example 1: disable storm control to broadcast packet

Raisecom#**config**

Raisecom(config)# **storm-control broadcast** *disable*

Raisecom(config)#**exit**

Raisecom#**show storm-control**

Broadcast: Disable

Multicast: Enable

Unicast destination lookup failed(DLF): Enable

Threshold: 1024 pps

Example 2: set storm control threshold value to 200kbps

Raisecom#**config**

Raisecom(config)# **storm-control** *bps 200*

Raisecom(config)#**exit**

Raisecom#**show storm-control**

Broadcast: Disable

Multicast: Enable

Unicast destination lookup failed(DLF): Enable

Threshold: 200 Kbps

Example 3: set storm control threshold to 2000.

Raisecom#**config**

Raisecom(config)# **storm-control** *bps 2000*

Raisecom(config)#**exit**

Raisecom#**show storm-control**

Broadcast: Disable

Multicast: Enable

Unicast destination lookup failed(DLF): Enable

Threshold: 2000 pps

Chapter 9 Layer-two Protocol

9.1 Layer-two protocol transparent transmission principle

QinQ offers a relatively simple layer-two VPN tunnel, by packaging outer layer VLAN Tag of user's private network message, so that the message is able to go through the operator's backbone network with layer-two Tag. Based on this, with layer-two protocol transparent transmission function, the layer-two protocol of the user's network can go through the operator's network, so that the same user network of the different places can run layer-two protocol in uniform.

Usually layer-two protocol transparent transmission is carried out by the operator's network edge switch. Transparent transmission function starts on the port that connect the operator's network edge switch and user network. The port exchange mode is access mode or dot1 q-tunnel mode, while the user switch port that is connected with it is trunk mode or hybrid mode. User network's layer-two protocol message, coming from the transparent transmission port, enters operator's network after being packaged by operator edge switch (message input interface). Then decapsulation will be done by the edge switch and the message will be transmitted to user network.

Transparent transmission function includes message packaging and decapsulation, the basic principle is shown below:

> ➢ Message encapsulation: in the message input side, the equipment will change the destination MAC address of layer-two protocol message from user network into special broadcast MAC address (default value 010E.05E00.0003). In operator network, the modified message will be transmitted in the user's VLAN as data message.
> ➢ Message decapsulation: in the message output side, the equipment will recognize the message that the destination MAC address is special broadcast MAC address (default value is 010E.5E00.0003), and revert the destination MAC address to the source destination MAC address of layer-two protocol message, then send the message to the given user network.

Layer-two protocol transparent transmission function can run with QinQ function or work respectively. But in actual, after the protocol message MAC address being modified, it still need to be covered with outer Tag to go through the operator network.

9.2 Layer-two protocol transparent transmission configuration

Layer-two transparent transmission configuration includes: transparent transmission protocol enable/diabale, transparent transmission message destination MAC address, COS value, the specified VLAN, the specified output port, message lost limit and port off limit. Configuring specified VLAN can make the transparent transmission message be transmitted by the specified VLAN, not the input VLAN; configuring the specified output port, can make the transparent transmission message being transmitted by only the given output port.

9.2.1 Layer-two protocol transparent transmission default configuration

Function	Default value
Enable/disable protocol transparent transmission	Disable
Message destination MAC address	010E.5E00.0003
Message COS	5
Specified VLAN	No specified VLAN
Specified output port	No specified output port
Message package lost limit	No limit
Message port disabled limit	No limit

9.2.2 Layer-two protocol transparent transmission configuration

By the following step, transparent transmission message destination MAC address, message COS value, the specified output port and VLAN can be configured, and enable/disable layer-two protocol transparent transmission function is available.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**relay destination-address** *HHHH.HHHH.HHHH*	Configure transparent transmission message destination MAC address, transparent transmission message destination MAC address must be broadcast address, and can not take 0x0180C2 or 010E.5E00.0003 as front
3 (optical)	**relay cos** *<0-7>*	Set transparent transmission COS value, range is 0-7
4	**interface port** *portid*	Enter Ethernet physical port mode
5	**relay port** *portid*	Set transparent transmission specified output port, range is 1-MAX port number.
6	**relay vlan** *<1-4094>*	Set transparent transmission message specified VLAN, range is 1-4094.
7	**relay** *{stp/dot1x/lacp/gmrp/gvrp/all}*	Enable/disable port layer-two transparent transmission function, all stands for all layer-two protocols that support transparent transmission.
8	**exit**	Return to global configuration mode
9	**exit**	Return to privileged EXECmode
10	**show relay**	Show transparent transmission function configuration and state
11	**write**	Save current system configuration

No relay destination-address reverts transparent transmission message destination MAC address to default value, that is 010E.5E00.0003. **no relay cos** clears transparent transmission message specified VLAN, that is the not specified VLAN. **no relay**{stp|dot1x|lacp|gmrp|gvrp|all} closes layer-two protocol transparent transmission function.

Notice：

➢ Transparent transmission message input equipment and output equipment need to configure the

same transparent transmission message destination MAC address, that is to say, to cooperate with other manufacturers, it is needed to keep the equipment transparent transmission message destination MAC address to stay the same. Transparent transmission message destination MAC address must be broadcast address, and can not begin with 0x0180c2 or 0x010E5E, but can be set to 010E.5E00.0003.

➢ Transparent transmission message COS value range is 0-7. Usually, transparent transmission protocol message PRI should be higher than ordinary data message.

➢ Transparent transmission specified output port can be any port of the equipment (except source port). User needs to make sure port VLAN attribution correct by configuration, or the message transparent transmission will fail.

➢ Transparent transmission specified VLAN value range is 1-4094. If this VLAN has not been created, transparent transmission message real-time transmission fails. So, when configuring specified VLAN, it is necessary to create and enable the VLAN on the equipment.

➢ To start layer-two protocol transparent transmission, it is needed to disable the corresponding protocols. To enable STP transparent transmission, closing STP protocol is needed.

➢ On the same equipment, when both the protocol message input port and output port transparent transmission function is enabled, the destination MAC address of protocol message will not be modified.

9.2.3 Layer-two protocol transparent transmission speed limit configuration

To configure transparent transmission message lost threshold and port off threshold, follow the steps below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** *portid*	Enter Ethernet physical port mode
3	**relay drop-threshold** *{stp	dot1x	lacp	gmrp	gvrp}* *<1-4096>*	Set transparent transmission message lost threshold, value range is 1-4096 PDUs/sec.
4	**relay shutdown-threshold** *{stp	dot1x	lacp	gmrp	gvrp}* *<1-4096>*	Set transparent transmission message close threshold, value range is 1-4096 PDUs/sec.
5	**exit**	Return to global configuration mode
6	**exit**	Return to privileged EXEC mode
7	**show relay**	Show transparent transmission configuration and state
8	**write**	Save the current configuration of the system

No relay drop-threshold *{stp|dot1x|lacp|gmrp|gvrp}*: revert transparent transmission protocol packet lost default configuration. **no relay shutdown-threshold** *{stp|dot1x|lacp|gmrp|gvrp}:* revert transparent transmission protocol port close threshold to default configuration, use **no relay shutdown** to enable the port.

Notice:

➢ Transparent transmission message packet lost threshold and port close threshold value range is 1-40%, usually, packet lost threshold should be less than port close threshold.

➢ After port transparent transmission function is enabled, if message receiving rate exceeds port close threshold, or if the port receives the message of specified destination MAC address, the port will be closed. When the port is closed because of transparent transmission function, use **no relay shutdown** to enable the port.

9.2.4 Layer-two protocol transparent transmission message statistics clear

Follow the step below to clear transparent transmission message statistics

Step	Command	Description
1	**config**	Enter global configuration mode
2	**clear relay statistics** [**port-list** *port-list*]	Clear transparent transmission message stat. information
3	**exit**	Return to privileged EXEC mode
4	**show relay statistics**	Show transparent transmission stat. information.

9.2.5 Monitoring and maintaining

Command	Description
show relay [**port-list** *port-list*]	Show transparent transmission configuration and state
show relay statistics [**port-list** *port-list*]	Show transparent transmission message stat. information

9.2.6 Typical configuration example
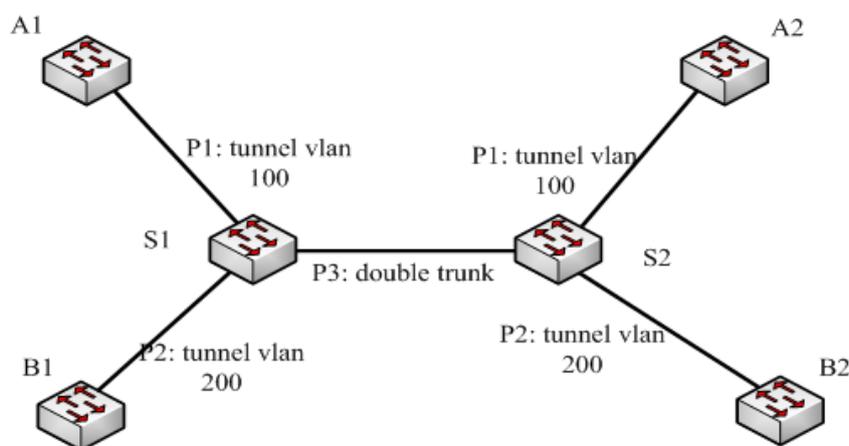
Fig 1 transparent transmission basic function configuration

S1,S2 configuration is the same. S1 configuration is shown below:

1) Create VLAN

Raisecom(config)#**create vlan** *100* **active**

Raisecom(config)#**create vlan** *200* **active**

2) Set port 1 exchange mode to dot1q-tunnel mode, ACCESS VLAN to 100, enable STP protocol transparent transmission and set STP message transparent transmission threshold to 1500.

Raisecom(config)# **interface port** *1*

Raisecom(config-port)#**switchport mode** d*ot1q-tunnel*

Raisecom(config-port)#**switchport access** vlan *100*

Raisecom (config-port)#**relay** *stp*

Raisecom(config-port)#**relay drop-threshold** *stp 1500*

Raisecom (config-port)#**exit**

3) Set port 2 exchange mode to dot 1q-tunnel mode, ACCESS VLAN to 200, enable STP protocol transparent transmission and set STP message transparent transmission threshold to 1000.

Raisecom(config)# **interface port** *2*

Raisecom(config-port)#**switchport mode** *dot1q-tunnel*

Raisecom(config-port)#**switchport access vlan** *200*

Raisecom (config-port)#**relay** *stp*

Raisecom(config-port)#**relay drop-threshold** *stp 1000*

Raisecom (config-port)#**exit**

4) Set port 3 exchange mode to trunk double-tagging mode.

Raisecom(config)# **interface port** *3*

Raisecom(config-port)# **switchport mode** *trunk double-tagging*

Raisecom (config-port)#**exit**

Chapter 10   Layer-Three Port

This chapter gives an introduction to how to configure and maintain the switch layer-three port, which includes:

✦   There-layer port introduction
✦   Layer-three port configuration
✦   Monitoring and maintaining
✦   Typical configuration example
✦   Layer-three port configuration debugging

10.1   Layer-three port introduction

ISCOM switch layer-three port is based on VLAN virtual port configuration, which is for network facility management. To the VLAN that needs router function, a related virtual layer-three port can be set for it. Layer-three port shows as IP address, and every layer-three port has a IP address and relate at least one VLAN.

10.2   Layer-three port configuration

At present, to ISCOM two-layer switch, 15 virtual layer-three ports can be configured, range is 0-14; to ISCOM layer-three switch, 63 virtual layer-three ports can be configured, range is 0-62.

The process of creating layer-three port and configuring IP address is shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	**Interface ip** *<0-ifNum>*	Enter Ethernet layer-three port configuration mode
3	**ip address ip-address** *[ip-mask] vlanlist*	Set layer-three port IP address and related static VLAN ID

10.3   Monitoring and maintaining

In privileged EXEC mode, use **show interface ip** to show layer-three port configuration state. By looking over the information shown, user can validate the configuration effect.

Command	Description
show interface ip *<0-ifNum>*	Show layer-three information

10.4   Typical configuration example

Set ISCOM switch IP port 1 address to 20.0.1.4, subnet mask to 255.255.255.0, and relate VLAN 1.

Raisecom #**config**

Raisecom (config)#**interface ip 1**

Raisecom (config-ip)#**ip address** *20.0.1.4 255.255.255.0 1*

10.5   Layer-three interface configuration debugging

Fault appearance: ISCOM switch can not connect the host by **ping**.

Debugging step:

Step 1: check out if the switch configuration is correct, use **show arp** to show if there is host ARP table unit in the ARP table.

Step 2: check out which VLAN the port that connect the switch and the host belongs to, if the VLAN belongs to the IP interface that is configured, if the IP address and the host belong to the same network segment.

Step 3: if the configuration is correct, open ARP debugging on-off on the switch, and check out if the switch has sent and receive ARP message correctly. If there is only message sent out, while no message received, then there may be problem in Ethernet physical layer.

Chapter 11   Link Aggregation

11.1   Link aggregation function principle

Link aggregation is to combine several physical Ethernet port into a logical aggregation group. Use the upper class entity of link aggregation service to take the physical links in the same aggregation group as a logical link.

Link aggregation is able to make the aggregation member taking part in the out/in traffic to increase bandwidth. At the same time, the member ports of the same aggregation group will dynamically backup each other, which increases the connection stability.

This chapter, trunk configuration includes:

> Enable/disable link aggregation.
> Add/delete link aggregation group
> Set all the aggregation link load-sharing mode

11.2 Static aggregation function configuration

11.2.1 Static aggregation default configuration

Function	Default value
Link aggregation	On
Link aggregation group	Does not exist, manual configuration is needed
Load balancing mode	Source, destination MAC address logic OR result selects the transmission port

11.2.2 Configure static aggregation

11.2.2.1   Configure aggregation group and start link aggregation function

Follow the following step to configure link aggregation:

Step	Command	Description
1	**config**	Enter global configuration
2	**trunk group** *trunk-group-id portlist*	Add a aggregation group; trunk-group-id the created aggregation group number, range is 1-6; Portlist physical port number list, use ',' and '-' to do multi-interface input
3	**trunk** *{enable|disable}*	Enable/disable link aggregation
4	**exit**	Quit global configuration mode and enter

		privileged EXEC mode
5	**show trunk**	Show if link aggregation is on, link aggregation load balancing mode, the group member port configured by all the aggregation groups and the effective member port

Use **no trunk group** *trunk-group-id* to delete the specified aggregation group.

In the same aggregation group, all the member ports that are able to share output/input load must be of the same configuration, which includes STP, QoS ,QinQ, VLAN, port attribution, MAC address learning, as is shown below:

Class	Contents
The same STP configuration	Port STP enable/disable state, link attribution that is connected with the port (port to port or not port to port), port path spending, STP priority, message sending out rate limit, configuring cycle protection or not, configuring root protection or not, edge port or not.
The same QoS configuration	Flow monitoring and shaping, jams avoidance, port traffic limit, SP line, WRR line attemperment.
The same QinQ configuration	Interface QinQ function on/off state, added outer layer VLAN Tag, the strategy of adding outer layer VLAN Tag that is different from inner layer VLAN ID.
The same VLAN configuration	The VLAN that is allowed to pass on the port, default VLAN ID of the port, the link type of the port (Trunk, Hybrid, Access), subnet VLAN configuration, protocol VLAN configuration, if there is Tag configuration in VLAN message.
The same port attribution	Whether to join isolate group, port rate, duplex mode, up/down state
The same MAC address learning configuration	Whether to own MAC address learning function, if the port has maximum learning MAC address limit, whether to continue transmitting and controlling when the MAC table is full.

11.2.2.2 Set load-sharing mode

Link aggregation has 6 load-sharing mode:

➢ **Smac** select transmission port according to source MAC address
➢ **Dmac** select transmission port according to destination MAC address
➢ **Axordmac** select transmission port according to source, destination MAC address logic OR result
➢ **Sip** select transmission port according to source IP address
➢ **Dip** select transmission port according to destination IP address
➢ **Sxordip** select transmission port according to source, destination IP address logic OR result

Step	Command	Description
1	**config**	Enter global configuration mode
2	**trunk loading-sharing mode** *{smac / dmac / sxordmac / sip / dip / sxordip}*	Configure all the link aggregation load-sharing mode
3	**exit**	Quit global configuration mode
4	**show trunk**	Show if link aggregation is on, link aggregation load-sharing mode, all the group

Use **no trunk loading-sharing mode** to revert link aggregation load-sharing default mode.

Notice: The command is supported by only a part of our equipments; follow the command manual for specific situation.

11.2.3 Monitoring and maintaining

Use **show** to look over link aggregation configuration

Command	Description
show trunk	Show if aggregation is enabled, link aggregation load-sharing balancing mode, all the group member port that is configured by aggregation group and the current effective member port.

Use **show trunk** to show if aggregation is enabled, link aggregation load-sharing balancing mode, all the group member port that is configured by aggregation group and the current effective member port. The current effective member port is the port list that the port state is UP in the configured group member ports. The example below is echo in the actual result:

Raisecom#**show trunk**

Trunk: Enable

Loading sharing mode: SXORDMAC

Loading sharing ticket algorithm: --

Trunk Group	*Member Ports*	*Efficient Ports*
3	*1,4-6,8*	*1,4*

11.2.4 Typical configuration example

11.2.4.1 Network requirement

SWA equipment use 4 ports aggregation to access SWB equipment, through which output/input load can be shared between the members. SWA access ports are port1~port 4.

11.2.4.2 Network structure
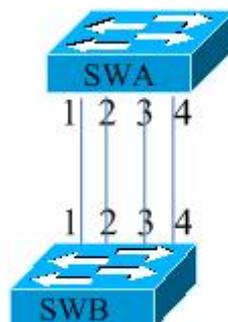
Fig 1 link aggregation network

11.2.4.3 Configuration step

Notice: The following steps list only the configuration to SWA; to SWB the same configuration is needed, so that link aggregation works.

1) Configure aggregation group, join the port into the aggregation group:

SWA#**config**

SWA(config)#**trunk-group** *1 1-4*

SWA(config)#set succesfully！

2) Configure the load-sharing mode of trunk link aggregation:

SWA(config)#**trunk loading-sharing mode** *smac*

SWA(config)#set succesfully！

3) Enable link aggregation function:

SWA(config)#**trunk enable**

SWA(config)#set succesfully！

SWA(config)#**exit**

SWA#**show trunk**

Trunk: Enable

Loading sharing mode: SMAC

Loading sharing ticket algorithm: --

Trunk Group	*Member Ports*	*Efficient Ports*
1	*1-4*	*1-4*

Chapter 12 STP

12.1 STP/RSTP principle introduction

12.1.1 STP purpose

STP (Spanning Tree Protocol) is founded according to 802.1D created by IEEE association, which is used for deleting data link layer physical loop protocol in local area network. The equipments that is running the protocol find loop in the network through exchanging message, and stop some ports selectively, then cut the loop network structure into tree network without any loop, which stop message breeding and looping endlessly, and avoid the host's message handling ability to decline because of receiving the same message.

STP has two meanings, narrowly-defined STP strands for the STP protocol defined in IEEE 802.1D, broadly-defined STP stands for the STP protocol defined in IEEE 802.1D and the modified spanning tree protocols based on it.

12.1.2 STP message

The protocol message STP uses is BPDU (Bridge Protocol Data Unit), which is also called configuration message.

STP transmits BPDU among equipments to make sure the network topology structure. There is enough information to make sure that the equipment finishes the spanning tree's computing.

BPDU is sorted into two types in STP:

- Configuration BPDU: the messages that is doing spanning tree computing and spanning tree topology maintenance.
- TCN BPDU (Topology Change Notification BPDU): the messages used for informing the related equipments network topology change when topology structure changes.

12.1.3 STP overview

1. root bridge

Root bridge is necessary for tree form network structure, so the concept of Root Bridge is taken into STP. There is only one root bridge all through the network, which changes according to network topology's change, so it is not stable.

After network convergence, the root bridge will create and send out configuration BPDU in accordance with a certain time interval, while the other equipments will transmit the configuration BPDU, to keep the topology stability.

2. root port

Root port means the port that is nearest to root bridge on a not-Root Bridge equipment, which sees to the communication to root bridge. There is only one root port on not-Root Bridge equipment, no root port on root bridge.

3. the designated bridge and port
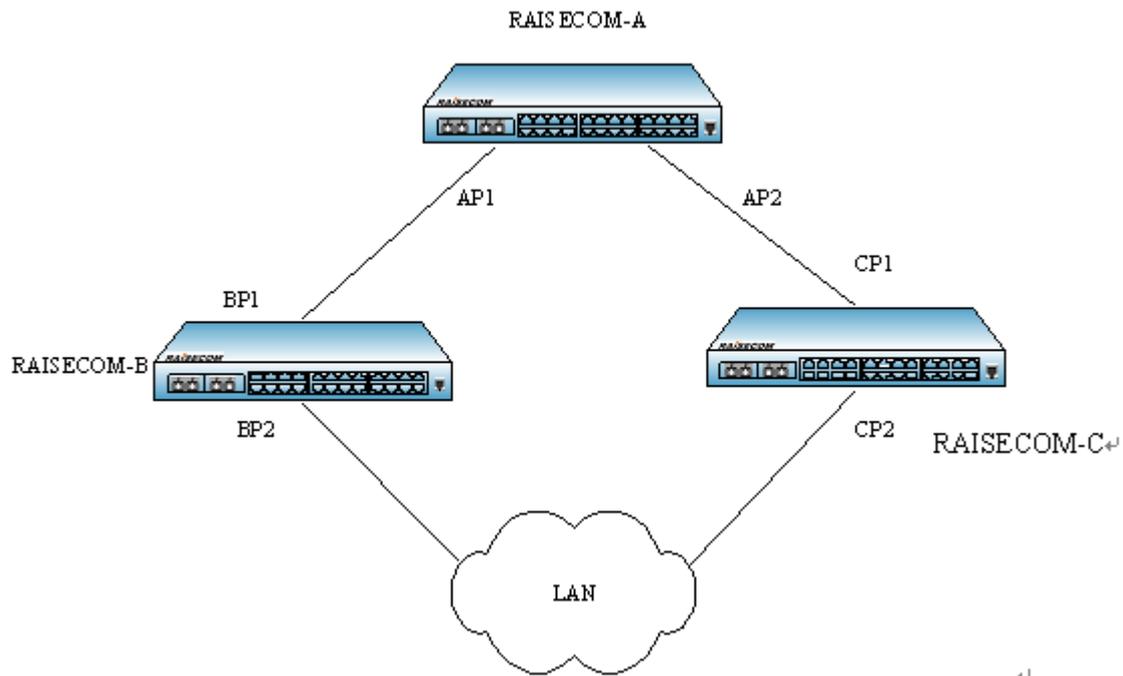
Fig 13-1: the designated bridge and prot

The designated bridge and port is shown above, AP1, AP2, BP1, BP2, CP1, CP2 stands for the ports of Device A, Device B, Device C respectively.

Device A uses port AP1 to transmit configuration message to Device B, then the designed bridge of Device B is Device A, the designated port is AP1 of Device A.

There are two equipments that connect local area network: Device B and Device C. If Device B sees to transmitting configuration messages to LAN, the LAN designated bridge is Device B, the designated port is BP2 of Device B.

Notice: all the ports on root bridge are designated ports.

4. path cost

Path cost is the reference value for STP selecting links. By computing path cost, STP chooses the 'strong' link, jams the redundant links and cuts the network into tree form network structure without any loop.

12.1.4 STP basic principle

STP algorithm:

➢ Initialized state:

Each equipment will generate the BPDU message information that take itself as root bridge when it is initialized, the path cost is 0, designates bridge ID as the equipment its own ID, and designated port is the local port.

➢ Optimal allocation information selection:

Each equipment sends out its own configuration information, and receives the configuration information of the other equipments. The process when each port receives configuration information is shown below:

- When the configuration information the port received is lower in priority than its own one, the equipment will drop the information received, and take no action to the port's configuration information.
- When the configuration information the port received is higher in priority than its own one, the

equipment will replace the configuration information content of its own with the received configuration information content.

- Compare all the ports' configuration information and select the optimal configuration information.

Configuration information compare principle:

- The smaller ID configuration information has higher priority;
- If root bridge ID is the same, compare the following configuration information priority and take the higher priority as the root bridge: the designed bridge ID, the designed port ID, the designed port ID, the port ID that receives the configuration information.

➢ Root bridge selection

When the network is initialized, all the STP equipments in the network will take themselves' root bridge, the root bridge ID is its own bridge ID. Through exchanging configuration information, the root bridge ID will be compared between the equipments, and the equipment that has the smallest root bridge ID in the network will be selected as the root bridge.

➢ Root port, the designed port selection

Root port is the port which has the least root bridge path cost, which is used for transmitting data to root node. If several ports have the same path cost to root bridge, the port that has the lowest port priority will be the root port.

Designated port: the port that transmits data to the downstream switch, at the same time sends STP message to maintain the spanning tree state.

STP configuration information transmission mechanism:

➢ When the network is initialized, all the equipments will take themselves as root bridge, and generate the configuration message that take themselves as root, then send the message out in the term of Hello Time;

➢ If the port that received configuration information is root port, and the received configuration information is higher in priority than the port configuration information, then the equipment will add Message Age which is taken in configuration message in a certain principle, and start timer to time this configuration, at the same time the configuration information will be transmitted from the designated port of the equipment.

➢ If the configuration message the designated port received is lower in priority than its own port's configuration message, it will send out better configuration message as response immediately.

➢ If there is fault on one path, the root port on the path will no longer receive any configuration information new, while the old configuration information will be dropped because of overtime, then the equipment will regenerate the configuration information that take itself as root and send out BPDU and TCN BPDU to trigger spanning tree's re-computing and get a new path to replace the faulted link, which will revert network connection.

However, the new configuration information getting from re-computing will not spread all through the network immediately, so the old root port and designated port will not realize the network topology change and continue transmitting data in the old path. If the newly selected root port and designated port start data transmitting immediately, provisional loop may happen.

STP timer:

➢ Forward Delay: the delay time of the switch state transformation. Link fault will trigger the network re-compute the spanning tree, and the spanning tree structure will change correspondingly. But the new configuration information that has just been re-computed will not spread all through the net immediately, if the newly selected root port and the designated port start data transmission immediately, it may bring temporary path loop. To stop it, STP take state transformation mechanism. The root port and designated port need to go through a betweenness stage before transmitting data, the stage can enter Forwarding stage only after two times Forward Delay time delay, which confirms that the configuration message has spread all through the network;

➢ Hello Time is used for detecting if there is fault in the link. The switch will send hello message out every Hello Time to check out if the link has any fault;

> ➤ Max Age is the parameter used to judge if the configuration information stored in the switch is 'out of time', the switch will drop the overtime configuration information.

12.1.5 RSTP principle overview

RSTP adds the mechanism that the port can transform from jam state to transmission state on the base of ordinary STP protocol, which quickens the topology convergence speed. In the pot to pot link that is connected with only two switch ports, proposal/agreement mechanism can be brought in and only the designated port's one handshake with downstream bridge, so that the link can be transformed quickly. The port that is connected directly to the terminal, not the other bridges, is defined as edge port, which can go directly into transmission state without out any delay. Because the bridge can not know if the port is connected with the terminal, manual configuration is needed.

12.1.6 STP related protocol and standard

The related protocol includes:

> ➤ IEEE 802.1D: Spanning Tree Protocol;
> ➤ IEEE 802.1w: Rapid Spanning Tree Protocol;
> ➤ IEEE 802.1s: Multiple Spanning Tree Protocol

12.2 Configure STP

12.2.1 Default STP configuration

Function	Default
Global STP function	Disable
Port STP function	Enable
STP and port priority	128
STP and system priority	32768
Network diameter	7
Port cost	Usually according to the physical feature the default value is shown below: 10Mbps: 2000000 100Mbps:200000 1000Mbps: 20000 10Gbps: 2000
The maximum package number every hello time	3
max-age timer	20s
hello-time timer	2s
forward-delay timer	15s

12.2.2 Root bridge/back-up root bridge

Step	Command	Description
1	**config**	Enter global configuration mode
2	**spanning-tree root {***primary, secondary***}**	Set the switch to root switch or back-up root switch for spanning tree
3	**exit**	Return to privileged EXEC mode
4	**show spanning-tree**	Show STP configuration

12.2.3 Port priority configuration

Step	Command	Description
1	**Config**	Enter global configuration
2	**interface port** *<1-MAX_PORT_NUM>*	Enter Ethernet physical port mode
3	**[no] spanning-tree priority** *<0-240>*	Set port priority for spanning tree
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show STP configuration

12.2.4 Switch priority configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**[no] spanning-tree priority** *<0-61440>*	Set the switch priority for spanning tree *0-61440* the switch priority
3	**exit**	Return to privileged EXEC mode
4	**show spanning-tree**	Show STP configuration

12.2.5 Path cost configuration

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** *<1-MAX_PORT_NUM>*	Enter Ethernet physical port mode *1-MAX_PORT_NUM* the equipment port number

3	[no] spanning-tree path-cost *<0-200000000>*	Set port inner path cost for spanning tree *0-20000000* port inner path cost
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show STP configuration

12.2.6 Maximum port transmitting rate configuration

Use this command to configure the maximum BPDU number that is allowed to be sent every Hello Time for MSTP. The parameter is a relative value, without any unit. The larger the parameter is set, the larger the message number that is allowed to be sent every Hello Time, and the more switch resource will be cost. Like time parameter, the configuration will take effect only in the root switch. By default, the value is 3. The configuration step is show below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**[no] spanning-tree transit-limit** *<1-10>*	Set the switch maximum sending rate
3	**Exit**	Return to privileged EXEC mode
4	**show spanning-tree**	Show MSTP configuration

12.2.7 STP timer configuration

> The switch has three time parameter: Forward Delay, Hello Time and Max Age:
> - Hello Time: the time interval of the switch sending the bridge configuration information (BPDU), which is used for the switch to detect if there is default with the link. Every Hello Time, the switch will send hello message to the switches around to make sure if there is default with the link.
> - The default value is 2s, user can change the value according to the network situation. When there are frequent changes in the network links, the value can be shortened to enhance the spanning tree protocol stability. Contrarily, enlarging the value will reduce the resource occupancy rate to system CPU of STP.
> - Forward Delay: confirm the time parameter of the switch's state transplant. Link fault will bring the network re-computing the spanning tree, and the STP structure will change accordingly, but the new configuration information by computing will not spread all through the network. If the newly selected root port and the specified port start data transmission immediately, provisional route cycle may happen. To prevent this, the protocol take a state transplant mechanism: the root port and designated port will have to go through a betweenness before data transmission, and only when the betweenness goes through Forword Delay can the ports enter transmission state. This delay confirms that the new configuration information has spread all through the network.

The default value is 15s, user can change it according to the situation, increase the value when the network topology change is not frequent, and decrease it on the contrary.

> - Max Age: the bridge configuration information that STP uses has lifecycle to judge if the configuration information is out of time. The switch will drop the outdated configuration information. When the bridge configuration information is out of time, the spanning tree protocol will re-compute the spanning tree.

The default value is 20s, a smaller value will result in the spanning tree re-computing much too frequent, while a value that is much too large will lead to the spanning tree protocol unfitness to the network topology structure change.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**[no] spanning-tree hello-time** *<1-10>*	Set the switch time parameter Hello Time
3	**[no] spanning-tree forward-delay** *<4-30>*	Set the switch time parameter Forward Delay
4	**[no] spanning-tree max-age** *<6-40>*	Set the switch time parameter Max Age
5	**exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show MSTP configuration

12.2.8 Configure edge port

12.2.9 STP mcheck operation

There are two working mode on the switch that supports MSTP: STP compatible mode and MSTP mode. If in a network the port of the switch that is running MSTP is connected with the switch that is running STP, the port will change into STP compatible mode automatically. But if the switch that is running STP is removed, the port can not change into MSTP mode automatically, but still works in STP compatible mode. Of course, if the port receives new STP message later, the port will return to STP compatible mode. The configuration step is shown below:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** *<1-MAX_PORT_NUM>*	Enter Ethernet physical port mode. *MAX_PORT_NUM* the maximum port number that the equipment supports.
3	**spanning-tree mcheck**	Force the port to move back to MSTP mode
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show MSTP configuration

12.2.10 Configure STP/RSTP mode switch

Step	Command	Description
1	**Config**	Enter global configuration mode
3	**spanning-tree mode{***stp/rstp/mstp***}**	Configure spanning tree work mode

4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show MSTP configuration

12.2.11 Configure link type

The two ports that is connected by point to point link can move to transmission state rapidly through transmitting synchronal message, which decreases unnecessary transmission delay time. By default, MSTP sets the link type of the port according to duplex state. Full duplex port is thought to be point to point link, while half duplex is thought to be shared link.

Users can configure by hand to force the current Ethernet ports and point-to-point link connected, but if the link point-to-point link is not a problem in the system would, under normal circumstances, the proposed user of this configuration is set automatically, by Automatic port discovery is linked with point-to-point link. Reverse order no spanning-tree link-type link state port to restore the default values. Specific configuration steps are as follows:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** *<1-MAX_PORT_NUM>*	Enter Ethernet physical port mode *MAX_PORT_NUM* the maximum port number that the equipment supports
3	**spanning-tree link-type** {*point-to-point / shared*}	Set the port's link type
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show MSTP configuration.

12.2.12 Statistics clear configuration

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** *<1-MAX_PORT_NUM>*	Enter Ethernet physical port mode *MAX_PORT_NUM* the maximum port number that the equipment supports.
3	**spanning-tree clear statistics**	Clear the port stat. information to zero
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show MSTP configuration

12.2.13 Monitoring and maintaining

Commands	Description
show spanning-tree	Show the basic information of spanning tree
show spanning-tree detail	Show the detailed information of the spanning tree
show spanning-tree port-list *[portlist]*	Show the basic information of the spanning tree port list
show spanning-tree port-list *[portlist]* **detail**	Show the detailed information of the spanning tree port list

12.2.14 Typical configuration instance

➢ There are 3 RAISECOM switch, A, B, C increase according to the equipment MAC address. By configuring the switch priority to select the root bridge to A or B freely, so that the topology can be changed;

➢ Network structure figure:
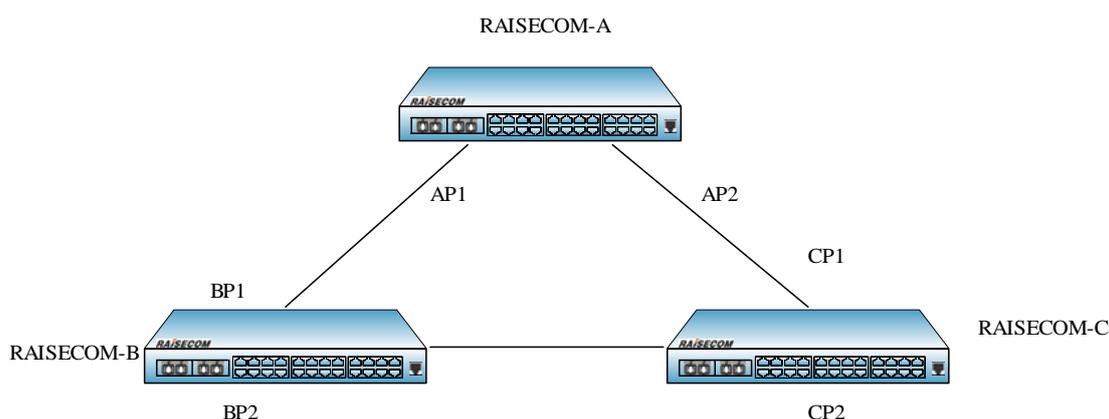
RAISECOM-A

Fig 13-2: network structure

➢ Configuration step:

Open A, B, C global STP:

Raisecom(config)#**spanning-tree** *enable*;

Set the STP working mode of port AP1, AP2, BP1, BP2, CP1, CP2 to RSTP;

By default, check out the stable topology structure:

Raisecom#**show spanning-tree**

A: the switch's AP1, AP2, as the designated port is in normal transmission state;

B: the switch's BP1, as the root port, is in normal transmission state, while BP2 is in block state;

C: the switch's CP1, as the root port, is in normal transmission state, while CP2 is in block state;

Set the priority of B to 4096, and repeat the following step:

Raisecom(config)#**spanning-tree priority** *4096*

When the topology is stable the root bridge will change into A, the port AP2, BP1 between A and c will be in block state.

MSTP configuration

12.3 MSTP principle introduction

12.3.1 MSTP overview

MST regions (Multiple Spanning Tree Regions), is made of several switches in the switch network and the network segments between them. These switches have all started MSTP, own the same domain name, VLAN to spanning tree mapping configuration and the same MSTP modification class configuration, and have physical link connection.

MSTI (Multiple Spanning Tree Instance) is the spanning tree in the MST domain. A MST domain can create several spanning trees through MSTP, each tree is independent.

VLAN mapping table is an attribution of MST domain. IST and CST (Common Spanning Tree) constitute the switch network spanning tree (Common and Internal Spanning Tree). IST is part of CIST in MST domain, which is a special multi-spanning tree instance.

CST is the simple spanning tree connecting all the MST domain in the switch network. If each MST is seen as a 'switch', CST is a spanning tree computed by the 'switches' using STP and RSTP.

CIST is a single spanning tree connected with all the MST domain in the switch network, which is formed by IST and CST.

Domain root means the tree root of IST and MSTI in the MST domain. The topology of each spanning tree in the MST domain is different, so the domain root may be different as well. Common Root Bridge means the tree root of CIST.

12.3.2 MSTP principle

MSTP divide the two-layer network into several MST domain, between each domain the CST is created by computing, while in the domain several spanning tree is created by computing by computing, each spanning tree is called a MSTI.

> The computing of CIST spanning tree

After comparing the configuration information, the switch that has the highest priority all through the network will be selected as the tree root of the switch. In each MST domain MSTP will create IST through computing, while MSTP will treat each MST domain as a single switch, and create CST in the MST domain by computing. CST and IST constitute the switch network CIST.

> MSTI computing

In the MST domain, according to the mapping relationship between VLAN and the spanning tree instance, MSTP will generate different spanning tree instance for different VLAN. Each spanning tree will make calculation respectively, the calculation process is similar with the process of STP/RSTP spanning tree computing.

> STP algorithm process

It is the same with STP/RSTP.

12.4 MSTP configuration

12.4.1 The default MSTP configuration

Function	Default value
Global MSTP function	Disabled
PORT MSTP function	Enabled
Max jump number of MST domain	20
The priority of STP port	128
The system priority of STP	32768
Network diameter	7
Port cost	According to the physical features, the usual situation by default is show below: 10Mbps: 2000000 100Mbps: 200000 1000Mbps: 20000 10Gbps: 2000
Max packet sent out number every Hello Time	3
max-age timer	20s
hello-time timer	2s
forward-delay timer	15s
MST domain modifying priority	0

12.4.2 MSTP domain configuration

When the switch running in MSTP mode, the switch can be configured the domain information where it belongs to. Which MST domain a switch belongs to is determined by the domain name, VLAN mapping table and MSTP modification configuration. By the following steps user can put the current switch into a special MST domain.

Annotation: MST domain configuration view is used here. To configure MST domain name, modification class and the relationship between VLAN and instances, it is needed to enter MST domain view. If the configuration is not enabled, then the configuration information will only be recorded but not activated. The configuration is shown below:

Step	Command	Description
1	config	Enter global configuration mode

2	**spanning-tree region-configuration**	Enter MST domain configuration mode
3	**[no] name** *name*	Set MST domain name
4	**[no] revision-level** *level*	Set MST domain modification class; Level: modification class, range is 0-65535, the default value is 0
5	**instance** *<0-4095>* **vlan** *<1-4094>*	Set mapping relationship from VLAN to instances for MST domain. 0-4095 the instance number; 1-4094 VLAN ID
6	**exit**	Return to global configuration mode
7	**spanning-tree region-configuration active**	Activate MST domain configuration information
8	**exit**	Return to privileged EXEC mode
9	**show spanning-tree region-configuration**	Show MST domain configuration information.

12.4.3 Configure MSTP domain maximum hop number

MST domain maximum hop number confines the scope of MST domain. Only when the configured switch is the domain root, can the configured maximum hop number be taken as MST domain maximum hop number, while other not-domain root switches configuration is not valid on it.

From the root switch of the spanning tree in the domain, BPDU in the domain hop number will decrease by 1 when transmitted by one switch, and the switch will drop the configuration information that receives 0 hop number. It will make the switch that is out of the max hop number not being able to take part in the spanning tree calculation, which confines the scope of MST domain.

For instance: if the maximum hop number of the domain root switch is set to 1, the spanning tree function in the domain is not available, because only this switch takes part in the spanning tree computing. By default, the maximum hop number is 20, or to hop down 19 steps along the spanning tree path from the domain root. The configuration is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**[no] spanning-tree max-hops** *<1-40>*	Set the maximum hop number of the switch MST domain
3	**exit**	Return to privileged EXEX mode
4	**show spanning-tree**	Show MSTP configuration

12.4.4 Configure root bridge/back-up root bridge

On the one hand, MSTP can configure the switch priority, and then after a spanning tree calculation, to

determine the root of the tree root switch to back up or exchange; On the other hand, the user can also specify the order directly. It should be noted that if the root switch designated direct way, then the whole network, users can not modify the proposed switch to any of the priority; Otherwise, the root cause designated switch or switch back up the root is invalid.

Users can instance instance-id parameter to determine the root switch, or switch to back up the root of the entry into force of instance. If the instance-id value is 0, or omit parameters instance instance-id, the current switch will be designated as the root of the CIST or switch to back up the root switch.

In the instance of the current switch in the type of root is independent of each other, that is, it can be used as an instance of the root switch or switch back up the root, at the same time as other instances of tree roots or switch to back up the root switch. But at the same instance of a tree, the same can not switch it as a root switch and root as a backup switch.

At the same time, the user can not be designated as an instance of spanning tree two or more root switch; On the contrary, the user can specify multiple spanning tree with a back-up roots. Under normal circumstances, the proposal for a user to specify a spanning tree roots and a number of back-up roots.

When the root switch failure or shutdown, the switch can replace the backup root root switch into the corresponding instance of the root switch. However, at this time if the user has set up a new root switch, then switch back up the root will not be a root switch. If a user to configure a number of instances spanning tree root switch back up, when the root switch fails, MSTP will choose the smallest of the MAC address of the switch as a backup root switch.

By default, the switch can not be taken as the root switch of the spanning tree or the back-up root switch of the spanning tree. Use **no spanning-tree[instance** instance-id**] root** revert command to restore the default configuration. Specific configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**spanning-tree** [**instance** *instance-id*] **root** {*primary, secondary*}	For a certain spanning tree instance, set the switch as the root switch or back-up root switch. *instance-id* instance number, range is 0-4095
3	**exit**	Return to privileged EXEC mode
4	**show spanning-tree**	Show MSTP configuration

12.4.5 Configure the port priority

Spanning tree protocol spanning tree calculation, the elections need to root port (root port) and designated ports (designated port), in the path of the port costs in line under the premise of the port-side ID of the smaller ports more vulnerable to root for the election or designated port. Users can set up port priority, to reduce port ID, and then there's the purpose of controlling spanning tree protocol to choose a specific port to become the root port or the designated port. With the same priority, the port that has smaller number has higher priority.

Same with the priority of configuring the switch, port priority is independent in different cases. Users can use **instance** instance-id parameter to determine the configuration of port-priority case. If the instance-id value is 0 or parameters **instance** instance-id is omitted, it is configured for the CIST port priority.

Note: The value of priority must be a multiple of 16, such as 0,16,32,48 and so on, the default value of 128.

Specific configuration steps are as follows:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** *<1-MAX_PORT_NUM>*	Enter Ethernet physical port mode; *MAX_PORT_NUM* the maximum port number that the equipment supports
3	[no] **spanning-tree** [**instance** *instance-id*] **priority** *<0-240>*	Set port priority for a certain spanning tree instance; *instance-id* instance number, range is 0-4095; 0-240 port priority value
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show MSTP configuration

12.4.6 Configure the switch priority

Bridge ID switch determines if the size of this switch can be selected as the root of the tree. Through the allocation of a smaller priority, the smaller switches Bridge ID can be got so that a certain switch can be the spanning tree root. Priority same, MAC address for the small roots.

Same with the configuration root and backup root, the priority is independent with each other in different instance configurations. Users can use **instance** instance-id parameter to determine the priority allocation of instance. If the instance-id value is 0, or when the parameters **instance** instance-id is omitted, it is configured for the CIST bridge priority.

Note: The value of priority must be in multiples of 4096, such as 0, 4096, 8192, and so on, the default value is 32,768. Specific configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	[no] **spanning-tree** [**instance** *instance-id*] **priority** *<0-61440>*	Set port priority for a certain spanning tree instance; *instance-id* instance number, range is 0-4095; 0-61440 port priority value
3	**exit**	Return to privileged EXEC mode
4	**show spanning-tree**	Show MSTP configuration

12.4.7 Configure the network diameter of the switch network

RSTP in the agreement, the network diameter refers to the number of switches in the network to exchange

up to the path that, switch the number of nodes. MSTP in the agreement, the network diameter settings only effective CIST for example MSTI invalid. And in the same region, no matter how many nodes path, just as a computing node. This fact, the network should be defined as the diameter across the domain up to that path, the number of domains. If the network has only one domain, then running network diameter is 1.

MST with the domain of the largest jump a few similar, if and only if the switch configuration for the CIST root switch, configure the entry into force.

Comparison of the MST's largest domain is used to jump a few domain characterization of the size of the network diameter is the characterization of the entire network of the size of a parameter. Network that the greater the diameter of a larger network.

When the user switches to configure the network parameters in diameter, MSTP through the switch will automatically calculate the Hello Time, Forward Delay, and Max Age three times to set the parameters for a better value.

Default network with a diameter of 7, the corresponding three time are their default values respectively. Specific configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**[no] spanning-tree bridge-diameter** *<2-7>*	Set the diameter of the switch network
3	**exit**	Return to privileged EXEC mode
4	**show spanning-tree**	Show MSTP configuration

12.4.8 Path cost configuration

When STP is computing the spanning tree, it is needed to vote root port and designated port, the less the port patch costs, the easier the port be voted as root port or designated port. Users can use **instance** instance-id parameter to determine the instance of the port inner path cost of the configured port. If the instance-id value is 0, or when the parameters **instance** instance-id is omitted, it is configured for the CIST inner patch cost.

Usually port cost depends on the physical features, the default case is:

➢ 10Mbps is 2000000;
➢ 100Mbps is 200000;
➢ 1000Mbps is 20000;

Specific configuration is as follows:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** *<1-MAX_PORT_NUM>*	Enter Ethernet physical interface mode MAX_PORT_NUM the maximum port number that the equipment supports
3	**[no] spanning-tree** [**instance** *instance-id*] **path-cost** *<0-200000000>*	Set the port inner patch cost for a certain spanning tree instance

		instance-id instance number, range is 0-4095
		200000000 the maximum patch cost value
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show MSTP configuration

12.4.9 Configure the port's maximum sending rate

Use the command to configure the maximum BPDU number that is allowed to be sent every Hello Time for MSTP. This parameter is a relative value, not units, the configuration parameters have been greater, each with Hello Time allowed to send the message, the more the number, but also will take up more resources to switch. With the same parameters of the time, only the root switch configuration comes into force.

By default, this value is 3. Specific configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**[no] spanning-tree transit-limit** *<1-10>*	Set the switch port maximum sending rate
3	**Exit**	Return to privileged EXEC mode
4	**show spanning-tree**	Show MSTP configuration

12.4.10 Configure STP timer

> There are three time parameter: Forward Delay, Hello Time and Max Age:
> - Hello Time: the time interval of the switch's sending BPDU, which is used to determine if there is fault in the link. Every Hello Time the switch will send hello message to the switches nearby to make sure if there is fault with the link.
> - The default value is 2s, user can change the value according to the network state. If there is frequent change in network links, the value can be shortened in a certain degree to enhance STP stability. On the opposite, enlarging the value will decrease STP resource taken rate to the system CPU.
> - Forward Delay: to make sure the time parameter of the switch state safe transformation. Link fault will bring in the re-computing of the spanning tree and the corresponding change of the network structure, but the new configuration information that is re-computed can not spread all through the network. If the newly elected root port and designated port started immediately transmit the data, may cause a temporary path of the loop. To this end an agreement to adopt a state transfer mechanism: the root port and designated port will go through a betweenness before data re-transmission (state of learning), a state in the middle Forward Delay after delay of time before they can enter the state forward. The delay to ensure that the new configuration information has been spread throughout the network.
> - Default value is 15 seconds, the user can adjust the value of the actual situation, when the network topology changes frequently are not able to reduce the value, increasing the contrary.
> - Max Age: the bridge configuration information that is used by the spanning tree protocol has life cycle to determine whether the configuration information is out of date. The switch will discard the configuration information out of date. When the bridge configuration information expired, spanning tree protocol will be re-spanning tree.

Default is 20 seconds, the value is too small will lead to weight spanning tree calculation too often, too

much will lead to spanning tree protocol in a timely manner can not adapt to the network topology.

The entire network to exchange all of the switches used CIST root switch on the three parameters of the time, only in the root switch configuration on the entry into force. Specific configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**[no] spanning-tree hello-time** *<1-10>*	Set the switch time parameter Hello Time
3	**[no] spanning-tree forward-delay** *<4-30>*	Set the switch time parameter Forward Delay
4	**[no] spanning-tree max-age** *<6-40>*	Set the switch time parameter Max Age
5	**exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show MSTP configuration

12.4.11 Configure edge port

Edge port: the port that has no direct connection to the switch or indirect connection to any switch through the network.

Configure the edge port so that the port state can transform into transmission state rapidly, without waiting for; for Ethernet port that is has direct connection with user's terminal equipment, it is supposed to be set to edge port for rapid transformation to transmission state.

If a port is set to edge port auto detection (auto), then the attribution of the edge port is decided by the actual situation. If a port is set to edge port (force-true), when the port receive BPDU the actual running value will become not-edge port, which will keep the state until the configuration is changed.

By default, all the network switch ports will be set to auto-detect. The reverse command **no spanning-tree edged-port** restores the default value of the edge port attribution. Specific configuration is as follows:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** *<1-MAX_PORT_NUM>*	Enter Ethernet physical port mode *MAX_PORT_NUM* the maximum port number that the equipment supports
3	**spanning-tree edged-port** {*auto	force-true	force-false*}	Set the edge port attribution.
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show MSTP configuration

12.4.12 STP mcheck operation

There are two working mode on switch ports that support MSTP: STP compatible mode and MSTP mode. Assuming an exchange network run MSTP switch port connected to the operation of the STP switches, the port will be automatically moved to the STP compatibility mode. However, at this time if the operation of the STP switch will be pulled away from the agreement, the port can not be automatically moved to the MSTP mode, STP will continue to work in the compatibility mode to run. At this point by **mcheck** operation it can be moved to MSTP mode. Of course, if later this port receives a new message STP again, the port will return to the STP compatibility mode. Specific configuration steps are as follows:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** *<1-MAX_PORT_NUM>*	Enter Ethernet physical port mode. *MAX_PORT_NUM* the maximum port number that the equipment supports
3	**spanning-tree mcheck**	Force the port to move to MSTP mode
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show MSTP configuration

12.4.13 Configure STP/MSTP mode switch

When STP is enabled, two spanning tree mode is supported: STP compatible mode and MSTP mode.

➢ STP compatible mode: do not implement the rapid transformation from alternate port to root port. Only STP configuration BPDU and topology change notice (STP TCN BPDU) will be sent out. The un-identified part will be dropped when MST BPDU is received.

➢ MSTP mode: sending MSTP BPDU. If the opposite end of the local switch port is running STP, the port will move to STP compatible mode. If the opposite end of the local switch port is running RSTP, the local will keep MSTP and take it only as out domain information.

The steps to configure the switch spanning tree mode are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**spanning-tree mode** {*stp*/*mstp*}	Set the spanning tree running mode
3	**exit**	Return to privileged EXEC mode
4	**show spanning-tree**	Show MSTP configuration

12.4.14 Configure link type

By transmitting synchronal message the two ports that is connected by point to point link can move to transmission state rapidly, which reduces the unnecessary transmission delay. By default, MSTP set the link type of the port according to duplex state. Full duplex port is seen as point to point link, while half duplex

port is seen as shared link.

Users can configure by hand to force the current Ethernet ports and point-to-point links connected, but the system will get into trouble if the link is not point to point link, usually it is supposed that this configuration is set to be auto so that the system will find out if the ports are connected with point to point link. Reverse command **no spanning-tree link-type** recovers the default value of the link state of the port. Specific configuration are as follows:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** <*1-MAX_PORT_NUM*>	Enter Ethernet physical port mode *MAX_PORT_NUM* the maximum port number that the equipment supports
3	**spanning-tree link-type** {*point-to-point* | *shared*}	Set the link type of the port
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show MSTP configuration

12.4.15 Configure static clear

MSTP counts each MSTP port BPDU message number of the following types: in STP message, in RSTP message, in MSTP message, out STP configuration message, out SRTP message (to the switch that is running MSTP, it will be zero forever), out MSTP message.

The steps to clear MST port statistics are as follows:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** <*1-MAX_PORT_NUM*>	Enter Ethernet physical port mode *MAX_PORT_NUM* the maximum port number that the equipment support
3	**spanning-tree clear statistics**	Clear the port statistics to zero
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode
6	**show spanning-tree**	Show MSTP configuration

12.5 Maintaining and management

 ➢ Show spanning-tree region-configuration: show MST domain configuration.
 ➢ Show spanning-tree [instance instance-id]: show multi-spanning tree instance basic information.
 ➢ Show spanning-tree [instance instance-id] detail: show multi-spanning tree instance detail.
 ➢ Show spanning-tree [instance instance-id] port-list[portlist]: show the basic information of

multi-spanning tree instance port list.
- ➢ Show spanning-tree [instance instance-id] port-list[portlist] detail: show the detail of multi-spanning tree instance port list.

12.5.1 Show instances

The result shown in the following sections are all according to the instance configuration described in the section, the switch that is for display is switch B in the example, the switch that uses this example is rc2828f (28 ports in all).

1. Topology voting figure and basic configuration

2. MST command configuration

Switch A:	Switch B:
Raisecom#**hostname** *SW_A*	Raisecom#**hostname** *SW_B*
SW_A#config	SW_B#config
SW_A(config)#create vlan 11-20 active	SW_B(config)#create vlan 11-20 active
SW_A(config)#interface port 1	SW_B(config)#interface port 27
SW_A(config-port)#switchport mode trunk	SW_B(config-port)#switchport mode trunk
SW_A(config-port)#switchport trunk allowed vlan 11-20	SW_B(config-port)#switchport trunk allowed vlan 11-20
SW_A(config-port)#exit	SW_B(config-port)#exit
SW_A(config)#interface port 2	
SW_A(config-port)#switchport mode trunk	SW_B(config)#interface port 28
SW_A(config-port)#switchport trunk allowed vlan 11-20	SW_B(config-port)#switchport mode trunk
SW_A(config-port)#exit	SW_B(config-port)#switchport trunk allowed vlan 11-20
	SW_B(config-port)#exit
SW_A(config)#spanning-tree enable	
SW_A(config)#spanning-tree mode mstp	
SW_A(config)#spanning-tree region-configuration	SW_B(config)#spanning-tree enable
SW_A(config-region)#name aaa	SW_B(config)#spanning-tree mode mstp
SW_A(config-region)#revision-level 2	SW_B(config)#spanning-tree region-configuration
SW_A(config-region)#instance 3 vlan 11-20	SW_B(config-region)#name aaa
SW_A(config-region)#exit	SW_B(config-region)#revision-level 2
SW_A(config)#spanning-tree region-configuration	SW_B(config-region)#instance 3 vlan 11-20
active	SW_B(config-region)#exit
	SW_B(config)#spanning-tree region-configuration
SW_A(config)#spanning-tree instance 0 priority 4096	active
SW_A(config)#spanning-tree instance 3 priority 8192	

	SW_B(config)#spanning-tree instance 0 priority 8192
	SW_B(config)#spanning-tree instance 3 priority 4096

12.5.2 Show MST domain configuration information

- ➢ Command: show spanning-tree region-configuration
- ➢ Function: to show MST domain configuration information, including: the inactive and valid domain, modification class and VLAN mapping table.
- ➢ Show result:

Raisecom#show spanning-tree region-configuration

Configured:

--

Name: aaa

Revision level: 2   Instances configured: 2

Instance   Vlans Mapped

--------   ----------------------

*   0   1-10,21-4094*

*   3   11-20*

Operational:

--

Name: aaa

Revision level: 2   Instances running: 2

Digest: 0x213106D1D279FAE00D24B8297D35EC69

Instance   Vlans Mapped

--------   ----------------------

*   0   1-10,21-4094*

*   3   11-20*

12.5.3 Show multi-spanning tree instance basic information

- ➢ Command: show spanning-tree [instance instance-id]
- ➢ Function: show all the spanning tree instances or the given spanning tree instance and the port basic information of the instance. Without the parameter instance instruction, all the instances and instance port information will be shown.
- ➢ Show the result:

Raisecom# show spanning-tree

MSTP Admin State: Enable

Protocol Mode: MSTP

MST ID: 0

BridgeId: Mac 000E.5E00.1864   priority 8192

Root: Mac 000E.83E3.7580   Priority 4096   ExternalRootCost 0

RegionalRoot: Mac 000E.83E3.7580   Priority 4096   InternalRootCost 200000

Operational: hello time 2, forward delay 15, max age 20

Configured: hello time 2, forward delay 15, max age 20

       transmit limit 3, max hops 20, diameter 7

PortId	PortState	PortRole	PathCost	PortPriority	LinkType	TrunkPort
1	discarding	disabled	200000	128	point-to-point	no
2	discarding	disabled	200000	128	point-to-point	no
3	discarding	disabled	200000	128	point-to-point	no
4	discarding	disabled	200000	128	point-to-point	no
5	discarding	disabled	200000	128	point-to-point	no
6	discarding	disabled	200000	128	point-to-point	no
7	discarding	disabled	200000	128	point-to-point	no
8	discarding	disabled	200000	128	point-to-point	no
9	discarding	disabled	200000	128	point-to-point	no
10	discarding	disabled	200000	128	point-to-point	no
11	discarding	disabled	200000	128	point-to-point	no
12	discarding	disabled	200000	128	point-to-point	no
13	discarding	disabled	200000	128	point-to-point	no
14	discarding	disabled	200000	128	point-to-point	no
15	discarding	disabled	200000	128	point-to-point	no
16	discarding	disabled	200000	128	point-to-point	no
17	discarding	disabled	200000	128	point-to-point	no
18	discarding	disabled	200000	128	point-to-point	no
19	discarding	disabled	200000	128	point-to-point	no
20	discarding	disabled	200000	128	point-to-point	no
21	discarding	disabled	200000	128	point-to-point	no
22	discarding	disabled	200000	128	point-to-point	no
23	discarding	disabled	200000	128	point-to-point	no
24	discarding	disabled	200000	128	point-to-point	no
25	discarding	disabled	200000	128	point-to-point	no
26	discarding	disabled	200000	128	point-to-point	no
27	forwarding	root	200000	128	point-to-point	no
28	discarding	alternate	200000	128	point-to-point	no

MST ID: 3

--

BridgeId: Mac 000E.5E00.1864   priority 32768

RegionalRoot: Mac 000E.5E00.1864   Priority 32768   InternalRootCost 0

PortId	PortState	PortRole	PathCost	PortPriority	LinkType	TrunkPort
27	forwarding	designated	200000	128	point-to-point	no
28	forwarding	designated	200000	128	point-to-point	no

12.5.4 Show multi-spanning tree instance detail

- ➢ Command: show spanning-tree [instance instance-id] detail
- ➢ Function: show all the spanning tree instances or the given spanning tree and the detail of the instance port. Without the parameter instance, all the instances and the detail of the instance port.
- ➢ Show the result:

Raisecom# show spanning-tree instance *0* detail

MSTP Admin State: Enable

Protocol Mode: MSTP

MST ID: 0

--

BridgeId: Mac 000E.5E00.1864   priority 8192

Root: Mac 000E.83E3.7580   Priority 4096   ExternalRootCost 0

RegionalRoot: Mac 000E.83E3.7580   Priority 4096   InternalRootCost 200000

Operational: hello time 2, forward delay 15, max age 20

Configured: hello time 2, forward delay 15, max age 20

transmit limit 3, max hops 20, diameter 7

Port 1 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 2 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 3 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 4 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 5 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 6 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 7 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 8 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 9 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 10 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 11 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 12 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 13 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 14 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 15 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 16 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 17 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 18 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 19 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 20 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 21 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 22 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 23 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 24 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 25 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 26 :

State:discarding   Role:disabled   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 0000.0000.0000   Priority 0   ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000   Priority 0   InternalPathCost 0

DesignatedBridge: Mac 0000.0000.0000   Priority 0   DesignatedPort 0

Port 27 :

State:forwarding   Role:root   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 000E.83E3.7580   Priority 4096   ExternalPathCost 0

RegionalRoot: Mac 000E.83E3.7580   Priority 4096   InternalPathCost 0

DesignatedBridge: Mac 000E.83E3.7580   Priority 4096   DesignatedPort 32769

Port 28 :

State:discarding   Role:alternate   Priority:128   Cost:200000   TrunkPort:no

Root: Mac 000E.83E3.7580   Priority 4096   ExternalPathCost 0

RegionalRoot: Mac 000E.83E3.7580   Priority 4096   InternalPathCost 0

DesignatedBridge: Mac 000E.83E3.7580   Priority 4096   DesignatedPort 32770

12.5.5 Show the basic information of multi-spanning tree instance port list

- ➢ Command: show spanning-tree [instance instance-id] port-list [portlist]
- ➢ Function: show all the spanning tree instances or the given spanning tree instance and the port basic information of the instance. Without the parameter instance instruction, all the instances and instance port information will be shown.
- ➢ Show the result:

Raisecom# show spanning-tree port-list *27*

Port ID:27

EdgedPort: admin: auto   oper: no

LinkType: admin: auto   oper: point-to-point

Partner MSTP Mode: mstp

Bpdus send:209   (TCN<0>   Config<0>   RST<0>   MST<209>)

Bpdus received:212   (TCN<0>   Config<0>   RST<212>   MST<0>)

Instance PortState   PortRole   PortCost(admin/oper) PortPriority

---

0   forwarding   root   200000/200000   128

3   forwarding designated   200000/200000   128

12.5.6 Show the detail of multi-spanning tree instance port list

- ➢ Command: show spanning-tree [instance instance-id] detail
- ➢ Function: show all the spanning tree instances or the given spanning tree and the detail of the instance port. Without the parameter instance, all the instances and the detail of the instance port.
- ➢ Show the result:

Raisecom# **show spanning-tree port-list** *28* **detail**

Port ID:28

EdgedPort: admin: auto   oper: no

LinkType: admin: auto   oper: point-to-point

Partner MSTP Mode: mstp

Bpdus send:241   (TCN<0>   Config<0>   RST<0>   MST<241>)

Bpdus received:243   (TCN<0>   Config<0>   RST<0>   MST<243>)

This port In mst0 Info:

State:discarding   Role:alternate   Priority:128   Cost: 200000

Root: Mac 000E.83E3.7580   Priority 4096   ExternalPathCost 0

RegionalRoot: Mac 000E.83E3.7580   Priority 4096   InternalPathCost 0

DesignatedBridge: Mac 000E.83E3.7580   Priority 4096   DesignatedPort 32770

This port In mst3 Info:

State:forwarding   Role:designated   Priority:128   Cost: 200000

RegionalRoot: Mac 000E.5E00.1864   Priority 32768   InternalPathCost 0

DesignatedBridge: Mac 000E.5E00.1864   Priority 32768   DesignatedPort 32796

12.6 Typical configuration instance

➢ Destination:

Set sw1, sw2, sw3 to the same MST domain MST1, modification class to 2, and map VLAN1 to instance 1, VLAN2 to instance 2, other VLAN to CIST;

Set MST2, MST3 to contain sw4/sw6/sw7, sw5/sw8/sw9, the correspondence that VLAN map to instance is similar to MST1.

Show the final spanning tree voting, configure the CIST that take sw3/sw4/sw5 as switch.

➢ Network figure
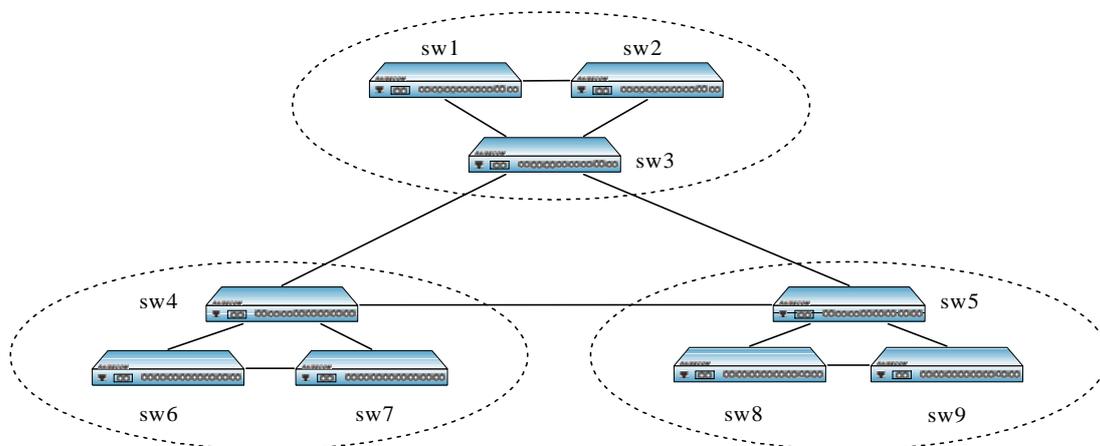
Fig 13-3 network figure

➢ Configuration step:

Step 1:

Configure MST domain configuration information, the domain name is MST, modification class is 2, map VLAN2 to instance 2, others to CIST, and enable the configuration information

Raisecom#**config**

Raisecom(config)#**spanning-tree region-configuration**

Raisecom(config-region)#**name** *MST1*

Raisecom(config-region)#**revision-level** *2*

Raisecom(config-region)#**instance** *1* **vlan** *1*

Raisecom(config-region)#**instance** *2* **vlan** *2*

Raisecom(config-region)#**exit**

Raisecom(config)#**spanning-tree region-configuration** *active*

Step 2:

Configure MST2 and MST3 in the same way.

Step 3:

To look over the spanning tree configuration information, instance 1 information:

Raisecom#show spanning-tree region-configuration

Raisecom#show spanning-tree instance 1

MST1, MST2, MST3 form as complete single spanning tree.

Step 4:

Set the electric physical port on MST1, MST2, MST3 domain to the member port of VLAN1;

In MST1 domain configure the bridge priority of sw3 to 4096, the priority of other switches larger than 4096;

In MST2 domain configure the bridge priority of sw4 to 8192, the priority of other switches larger than 8192;

In MST2 domain configure the bridge priority of sw5 to 8192, the priority of other switches larger than 8192;

In each domain, the topology will vote and create single spanning tree according to STP/RSTP, and create a final tree, the root of which is sw3, and the connection between sw4 and sw5 will be stopped.

There is only one MST1 in MST1/MST2/MST3 domain, sw3/sw4/sw5 is thought to be root, the topology picture is as follows:

Fig 13-4 topology figure

Chapter 13   Unicast Router
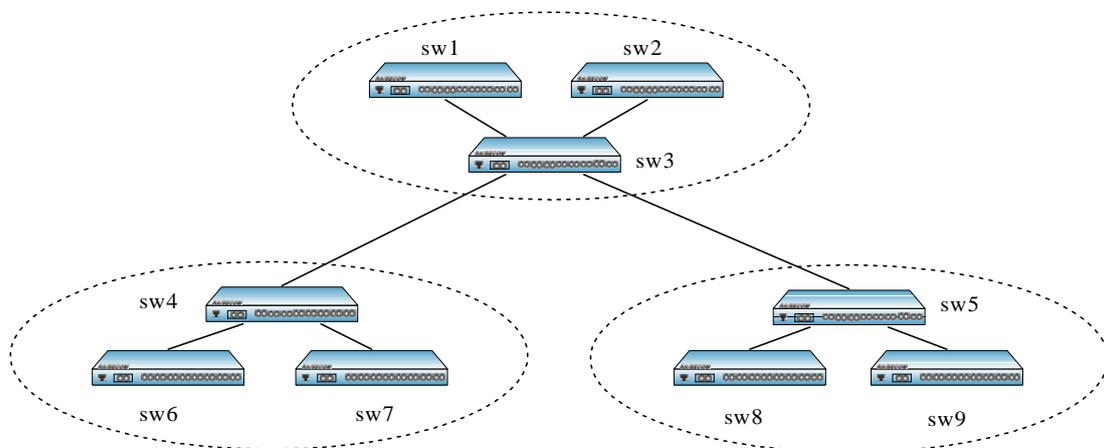
13.1 Routing Overview

13.1.1 Overview

If there is no L3 device between VLANs, the devices which are in different VLAN can not communicate with each other. There are three kinds of routing.

- ➢ Default routing;
- ➢ Static routing;
- ➢ Dynamic routing.

A default routing is a special routing. You can configure a default routing using a static routing.

A static routing is a special routing configured manually by an administrator.

The advantage of static routing that it's safe and saves bandwidth, but can not adapt the dynamic change of network topology structure, like link invalidation and so on, so it may cause the destination unreachable. As network topology spreads, static routing will cost much time and energy.

Routing use dynamic routing protocol, which is able to compute the best routing for data stream. There are two types of dynamic routing protocol:

1. Use distance vector protocol to maintain routing table, it takes the distance of network resource as the computing evidence, and it can send routing table to neighbours periodically. Distance vector protocol uses one or one serious metric to compute the best routing, which makes it more convenient for configuration and usage.

2. Use link state protocol to maintain the data-base of network topology, that is to exchange link state announces (LSAs) among routings for maintenance. Sending LSAs is touched off by incidents, like constringency timer overtime or receiving request timer overtime. Link state protocol is able to answer the topology changes rapidly, but it needs more bandwidth and resources compared with distance vector protocol.

The distance vector protocol that ISCOM three-layer switch supports is RIP, which uses metric to choose the best routing. At the same time, the switch also supports open frame shortest path first link state protocol.

In some network environment, VLAN connects to different network or subnet. In IP network, each subnet is mapped to a signal VLAN. VLAN configuration is about to control the size of broadcasting domain. However, when one VLAN end needs to communicate with the end in another terminal, the communication between VLAN- routing among VLAN is needed. You can configure one or more routing to transmit data stream to each destination VLAN.

Figure 1-1 shows basic routing topology structure, switch A is in VLAN 1, switch B is in VLAN 2, routing has a port in each VLANA. When host A in VLAN 1 needs to communicate with host Bin VLAN 1, it sends out a data packet, the destination address is host B, the switch will transmit the data packet directly to host B, without sending to routing. When host A sends data packet to host C in VLAN 2, switch A will transmit the data packet to routing. The routing will receive the packet on the port in VLAN 1, check out routing table, choose the correct outgress port, and send the data packet to the port of switch B on VLAN 2. Switch B will receive the data packet and transmit it to host C.
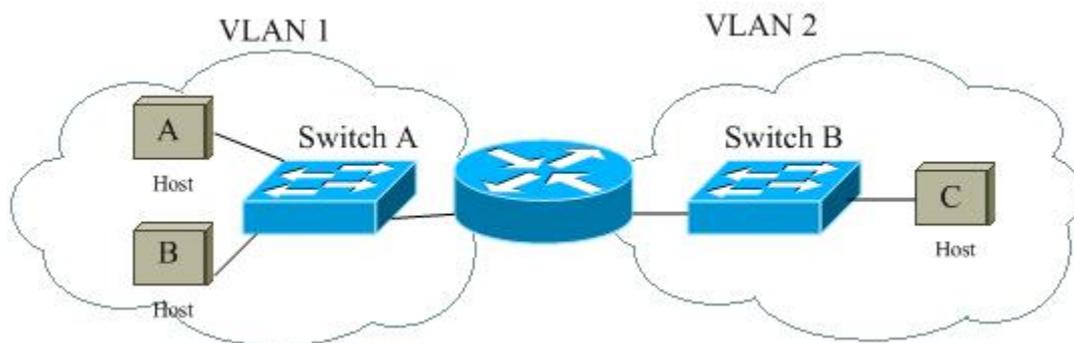
Fig 1-1 basic routing topology structure

13.1.2 Enable routing transmission

To realize three-layer routing transmission, **ip routing** is needed. By default the system forbids any software transmitting IP message. Enable IP transmission function, it is only needed to do the following configuration in global configuration mode. Use **no ip routing** to restore default configuration.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip routing**	Enable/disable IP routing transmission function

Notice: Before you use the layer-3 function like static routing, dynamic routing and default gateway, IP routing transmission function must be opened first.

13.2 Static Routing Configuration

13.2.1 Static routing overview

13.2.1.1 Static routing

Static routing is a special routing, it is manually configured by the administrator. By configuring static routing a communicating network can be established.

The advantage of static routing is safety and bandwidth saving. In the network with simple structure, it is only needed to configure static routing to make routing work, proper configuration and usage of static routing can improve the performance of network and offer enough bandwidth for important application. However, static routing can not adapt the dynamic change of network topology structure automatically, like unavailable link, so it may the destination is unreachable. As the growth of network topology, static routing will waste more and more time and energy.

13.2.1.2 Default routing

Default routing is a special routing. In brief, default routing is the routing that will be used only when there is no corresponding table item. That is, only when there is no proper routing, can default routing be used. In the routing table, default routing can appear with the address 0.0.0.0 (mask 0.0.0.0). Use **show ip routing** to check out if it is configured. If the destination address can not match up with any table item in the routing

table, the message will be selected as default routing. If there is no default routing while the message destination is not in the routing table, then when the message is dropped, a ICMP message will be returned to the source end to report that the destination or network is unreachable.

13.2.2 Configure static routing

13.2.2.1 Default static routing configuration

Function	Default value
Static routing	Empty
Default routing	empty

13.2.2.2 Configure static routing

Sometimes, for simple network, the administrator can configure static routing manually. The process is as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip routing** *10.0.0.0 255.0.0.0 192.168.1.1*	Set the IP address of the next hop to destination network 10.0.0.0 is 192.168.1.1
3	**exit**	Return to privileged EXEC mode
4	**show ip routing**	Show routing table
5	**config**	Enter global configuration mode
6	**no ip routing** *10.0.0.0*	Delete the routing in 10.0.0.0 network
7	**exit**	Return to privileged EXEC mode
8	**show ip routing**	Show routing table

When using **no ip routing**, network mask can be designated, and it can be undesignated to default mask. The next hop of routing must be the routing in the straight-through network.

13.2.2.3 Default gateway configuration

When a message that is needed for transmission do no find the destination network routing, use **ip default-gateway** to let the system transmit all the messages to default gateway. The steps are shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip default-gateway** *192.168.1.1*	Configure default gateway

3	**exit**	Return to privileged EXEC mode
4	**show ip routing**	Show routing table
5	**config**	Enter global configuration mode
6	**no ip default-gateway**	Cancel default gateway configuration
7	**exit**	Return to privileged EXEC mode
8	**show ip routing**	Show routing table

Notice: For successful configuration, configure IP address is needed first, or configuring default gateway will be failed.

13.2.3 Monitoring and maintenance

Show routing table commands:

Command	Description
show ip routing	Show routing table

13.2.4 Typical configuration example

1) Network request

Configure static routing so that any two hosts or switches can PING through each other. The switch in the figure below is three layer switch

2) Topology

PC C   Gateway 10.1.5.3

Interface 3
10.1.5.3/24

Interface 1   Interface 2
10.1.2.3/24   Swith A   10.1.3.3/24

Interface 1   Interface 1
10.1.2.4/24   10.1.3.4/24

Interface 2   Swith B   Swith C   Interface 2
10.1.1.3/24   10.1.4.3/24

PC A   Gateway 10.1.1.3   PC B   Gateway 10.1.4.3
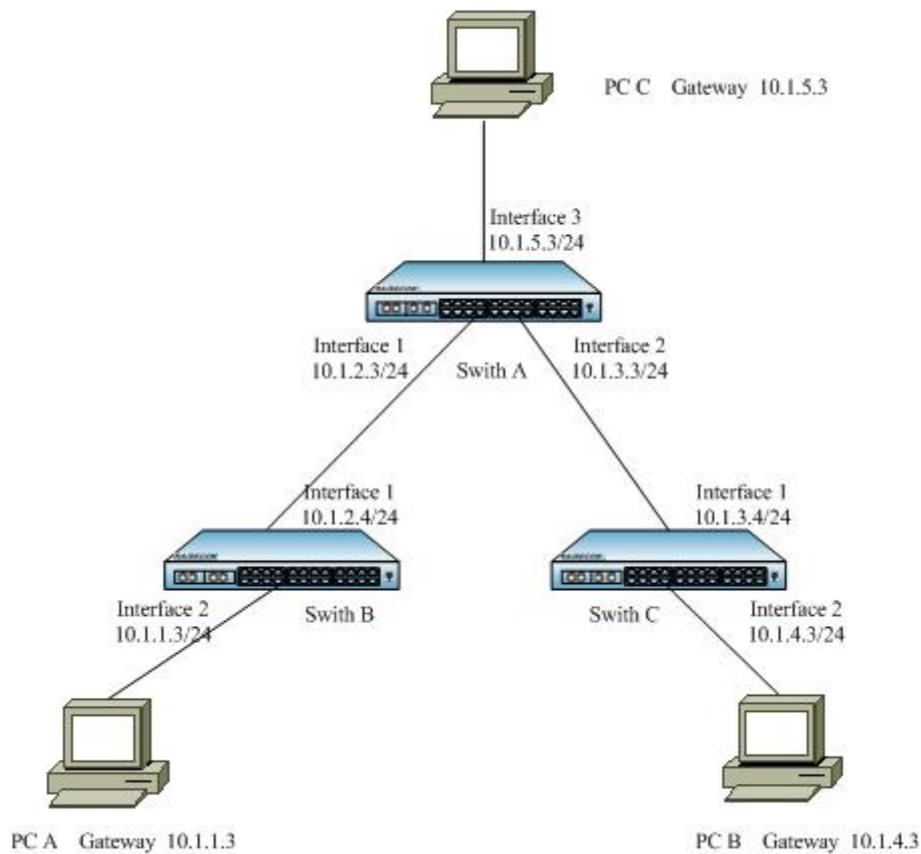
Fig 2-1 static routing configuration network structure

3) Configuration step

The precondition is to configure the IP address of each interface.

! Enable ip routing on Switch A and configure default gateway

Raisecom(config)# **ip routing**

Raisecom(config)# **ip routing** *10.1.1.0 255.255.255.0 10.1.2.4*

Raisecom(config)# **ip routing** *10.1.4.0 255.255.255.0 10.1.3.4*

! Enable ip routing on Switch B and configure default gateway

Raisecom(config)# **ip routing**

Raisecom(config)# **ip default-gateway** *10.1.2.3 255.255.255.0*

! Enable ip routing on Switch C and configure default gateway

Raisecom(config)# **ip routing**

Raisecom(config)# **ip default-gateway** *10.1.3.3 255.255.255.0*

! Configure default gateway to 10.1.1.3 on host A, the detailed configuration is omitted

! Configure default gateway to 10.1.4.3 on host B, the detailed configuration is omitted

! Configure default gateway to 10.1.5.3 on host C, the detailed configuration is omitted

Up till now any two hosts or Ethernet switches in figure 2-1 can make connection with each other.

13.2.5 Static routing troubling shooting

Trouble phenomena: the physical connection is correct, but they can not ping through each other

Trouble shooting:

Step 1: check out if the IP address of each port is correct.

Step 2: use **show ip routing** to check out if static routing or default gateway configuration is available.

Step 3: use **show running-config** to check out if routing transmission is enabled.

13.3 RIP Configuration

13.3.1 RIP overview

Rip: Routing Information Protocol.

RIP is one of the most widely used interior gateway protocols now, which takes the famous distance vector algorithm. RIP is the simplest kind in distance vector protocol family, its routing choice is mainly based on the hop number before reaching destination spot, and usually this is weighed by the size of metric. RIP takes the distance from routing to its straight-through network is 0 hop, metric value is 1; the routing that needs to go through a routing is 1 hop, metric value is 2; the rest are like this. The maximum path cost that RIP supports is 15; when metric is larger than 16, RIP takes the path cost as infinite, and destination network is unreachable.

RIP is the protocol based on UDP (user datagram protocol) data message. The gateway or host that is running RIP needs to use 520 port of UDP to receive/send out messages when doing routing exchange. In RIP protocol, each routing that takes routing exchange will send out routing update messages to neighbor routings 6 after a certain period (30s by default). If the routing does not receive routing update information after about 6 update periods(180s by default), the link will be taken as unavailable. If in a certain time followed (300s by default) there is still no update information received from the link, it will be deleted from the routing table.

To improve the performance and make effective reflection in time to network topology structure, RIP protocol supports plant division, which saves a lot of shrinking time. At the same time, use trigger update for routing information change.

Raisecom three layer switches support both RIPv1 and RIPv2. RIPv2 supports clear text authentication, alterable long mask and classless inter-domain routing selection.

13.3.2 Configure RIP

To enable RIP layer-3 interface need to be configured for each network segments, use **ip routing** to realize three layer routing transmission function.

13.3.2.1 Default RIP configuration

Function	Default value
RIP routing protocol	Disabled
The given network RIP protocol	Disabled
RIP message receiving version	v1v2
RIP message sending version	broadcastv2
Port RIP protocol authentication mode	No authentication
Port add-ons measurement value configuration	1
RIP routing deleting timer exceed time	300 seconds
RIP invalid timer	150 seconds
RIP update timer	30 seconds

13.3.2.2 Start RIP

Use **routing rip** to start RIP protocol. Enabling RIP protocol is the precondition of all the other RIP configuration. Follows the commands below in global configuration mode:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**routing rip**	Enable RIP

13.3.2.3 Enable the RIP protocol specified network

Use **network** to start RIP protocol of the given network, when the specified network and port IP address are in the same network, you can enable the port for RIP messages' receiving/sending. You can configure port IP address first, then use **network** to specify the network enabling port RIP protocol, and begin receiving/sending RIP messages; you can also use **network** to specify a network, then configure corresponding network IP address for the ports to enable port RIP protocol and begin receiving/sending RIP messages. When in a specified network, you need to specify the corresponding network mask at the same time. On a switch, the number of the network that is specified with **network** is unlimited. Use **no network** to clear the configuration. Follow the commands below for specified operation:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**routing rip**	Enable RIP and turn to protocol configuration mode
3	**network** *network-number netmask*	Enable RIP protocol of the specified network

13.3.2.4 Configure RIP version

ISCOM allow you change some configuration parameters on the port, use **ip rip receive-version** to configure the version of RIP messages that be received by current port. You can ignore a certain version and do not handle it. When the port is configured to receive RIPv2, RIPv1 messages need not to be received. When the port is configured to receive *donotreceive*, the port will not receive rip messages. By default, the version of the RIP messages that can be received by current port can be configured as all. Use **no ip rip receive-version** to restore default configuration. Use **ip rip send-version** to configure the version of the RIP messages that current port can send out. By default, only version 1 RIP message can be sent out from current port, and when the port is configure to receive *donotsend*, any RIP message can be sent out from the port. Use **no ip rip send-version** to restore current port sending version to default version.

Specified operation is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** *ifNum*	Switch to three layer interface configuration mode
3	**ip rip receive-version** *{ v1 / v2 / v1v2 / donotrecieve }*	Configure the version of the RIP message that can be received by current port
4	**ip rip send-version** *{ v1 / multicastv2/broadcastv2/donotsend }*	Configure the version of the RIP message that can be received by current port

13.3.2.5 The authentication mode of port RIP protocol

ISCOM allows configure man to change the authentication method of RIP interface protocol, but to all the routings that is connected with the same network, the validation and password must keep the same, otherwise the routing may lose connection between each other. Use **ip rip auth-mode** to configure the authentication mode of current RIP protocol or it does not need authentication. Only RIPv2 supports authentication, while RIPv1 does not, but RIPv1 can be configured success. **No ip rip auth-mode** can help restore default configuration.

In interface configuration mode, the authentication mode of interface RIP protocol can be change in the following way:

step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** *ifNum*	Switch to three-layer interface configuration mode
3	**ip rip auth-mode** *{none/text}*	Configure the interface RIP protocol validation access

13.3.2.6 Configure port additional metric value

Use **ip rip metric-default** to configure the additional metric value that current port gives to received RIP routing, which stands for the price that the routing needs to take when going through the node. User can change the configuration according to the need. Use **no ip rip default-metric** to restore it to default value.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** *ifNum*	Switch to three-layer interface configuration mode
3	**ip rip metric-default** *value*	Configure port additional metric value

13.3.2.7 Configure RIP timer

Use **timer flush** to configure the invalidation cycle of RIP routing that all the ports receive, which is the waiting time the routing changes from invalid to being deleted. Use **no timer flush** to restore it to default value.

Use **time invalid** to configure the life cycle of RIP routing that all the ports receive, which is the waiting time the routing changes from invalid to being deleted. Use **no timer invalid** to restore it to default value.

Use **timer update** to configure the update cycle of all the ports' sending RIP messages and change the frequency that current port sending cycle update messages. Use **no timer update** to restore it default value.

To configure RIP timer, follow the steps below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**routing rip**	Switch to RIP protocol configuration mode
3	**timer flush** *timeout*	Configure the waiting time that routing changes from invalid to being deleted
4	**timer invalid** *timeout*	Configure the waiting time that routing changes from received to invalid
5	**timer update** *timeout*	Configure the update cycle of all the port's sending RIP messages

Notice: When configuring RIP timer, notice the network performance before you change the value of timer, and make uniform configuration to all the routings that are running RIP, to avoid unnecessary network flow or network rout shake.

13.3.2.8 Configure RIP split-horizon

Split-horizon mechanism stops routing information from going back to the sending direction. You can describe split-horizon like this: if the port that sends RIP routing is the same one that receives RIP routing, then the routing metric value needs to be set infinite before being sent out. Thus, it can prevent network rip from coming into being., and tell neighbor equipments the information that what is unreachable in time, which saves the shrinking time. While broadcasting a invalid routing with 16 path cost will bring in additional information. By default, current port RIP has started split-horizon mechanism. Use **no ip rip split-horizon** to close port split-horizon mechanism.

To configure RIP timer, the operations are shown below:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**interface ip** *ifNum*	Switch to three-layer interface configuration mode
3	**no ip rip split-horizon**	Disable port split-horizon mechanism

13.3.3 Monitoring and maintenance

Use some **show** commands to look over routing running situation, the content of routing table and the state of routing protocol and so on, for the convenience of monitoring and maintenance. Follow the commands below to make it:

Commands	Descripton
show ip route	Show routing table
show ip protocol	Show routing protocol and the routing protocol configuration state under port
show ip rip statistics	Show RIP protocol and port static information

Use **show ip route** to check out if RIP connection is normal, and look over RIP routing state to check out if RIP communication is normal.

Raisecom# **show ip route**

Codes: C - Connected, S - Static, R - RIP, O – OSPF

--

C   20.1.1.0[255.255.255.0],is directly connected , Interface 1

C   30.1.1.0[255.255.255.0],is directly connected , Interface 2

R   40.1.1.0[255.255.255.0],Via 30.1.1.4

R   50.1.1.0[255.255.255.0],Via 30.1.1.5

Total route count: 4

When RIP connection is established normally, the router will learn corresponding RIP routing, and two routes ahead with R will be shown in the routing table. A RIP routing contains the following information:

1. How router get information (R-from RIP protocol);

2. Destination network and the corresponding mask;

3. The next hop of router (across 30.1.1.4 or 30.1.1.5);

Use **show ip protocol** to look over the configuration information of the routing protocols like OSPF, RIP and so on. When RIP protocol get started, it will inform RIP protocol configuration information, the RIP configuration state of each port, appoint network list and protocol priority for RIP selection router; when RIP protocol is disabled, no information about RIP protocol will be shown. To help use the command, let's take RouterA in figure 3-1 for example an see how it works:

Raisecom#**show ip protocol**

The system will return:

Routing Protocol is 'RIP'

RIP global Enable

Default version control: send version 2(broadcast),   receive any version

RIP supply interval is 30 (default 30)second

RIP router expire interval is 180 (default 180)second

RIP router flush interval is 300 (default 300)second

IF	Send	Recv	Metric	Split	Auth-mode	Auth-key	State
1	*2(B)*	*1 2*	*1*	*Enable*	*none*		*UP*
2	*2(B)*	*1 2*	*1*	*Enable*	*none*		*UP*

Routing for Networks:

20.1.1.0	*0.0.0.255*	*active*
30.1.1.0	*0.0.0.255*	*active*

Distance(default is 120):120

To the message and route send and received by RIP, use the command below for detail:

Raisecom#**show ip rip statistics**

The system will return:

Num of routes   changed   :8

Num of responses sent to RIP queries   :0

interface 1:

The address of this interface is :20.1.1.3

Num of packets   discarded   :0

Num of routes   discarded   :0

Num of triggered updates   :1

interface 2:

The address of this interface is :30.1.1.3

Num of packets   discarded   :0

Num of routes   discarded   :0

Num of triggered updates   :1

13.3.4 Typical configuration example

1) Topology figure
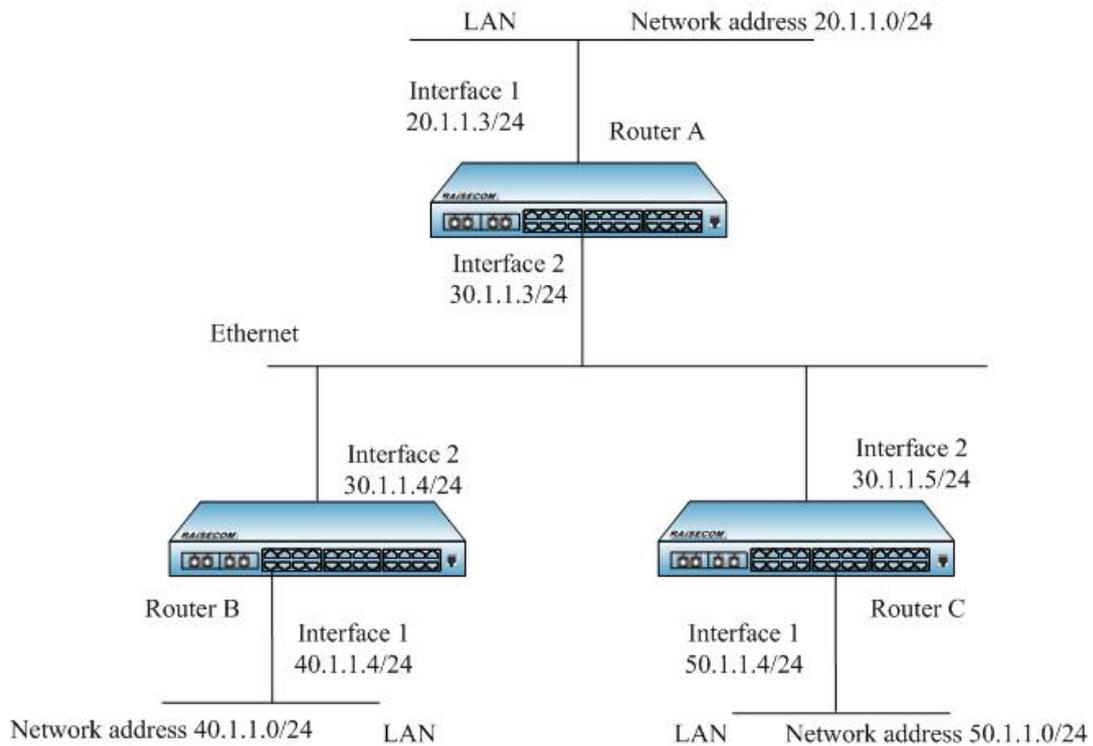
Fig 3-1 RIP configuration example (network structure show)

2) Configuration instruction

As is shown in figure 3-1, RouterA connects to subnet 20.1.1.1/24 using Ethernet port. RouterB, RouterC Ethernet ports connect to 40.1.1.0/24 and 50.1.1.0/24 respectively. RouterC, Router A and Router B are connected using Ethernet 30.1.1.0/24. Follow the figure to configure IP port and port address.

3) Configuration steps

The steps below are only about the operation related with RIP.

! Enable ip routing

Raisecom(config)# **ip routing**

! Configure Router A

Raisecom(config)# **router rip**

Raisecom (config-router-rip)# **network** *20.1.1.0   0.0.0.255*

Raisecom (config-router-rip)# **network** *30.1.1.0   0.0.0.255*

! Configure Router B

Raisecom(config)# **router rip**

Raisecom (config-router-rip)# **network** *30.1.1.0   0.0.0.255*

Raisecom (config-router-rip)# **network** *40.1.1.0   0.0.0.255*

! Configure Router C

Raisecom(config)# **router rip**

Raisecom (config-router-rip)# **network** *30.1.1.0   0.0.0.255*

Raisecom (config-router-rip)# **network** *50.1.1.0   0.0.0.255*

13.3.5 RIP trouble shooting

Fault: the physical connection is normal, but the RIP protocol communication between each other is incorrect.

Fault shooting:

Step 1 use **ping** to test if network connection is normal.

Step 2 if it is normal, use **show ip protocols** to examine if RIP has been started normally on both sides, and check out if RIP protocol is valid, if port RIP protocol has been started, that is to check out if the network that port IP address belongs to is in the list appointed by **network**.

Step 3 check out if the configuration about validation on both sides are consistent. If there are validations on both sides, check out if the passwords are same.

Step 4 check out the version limit of sending & receiving RIP messages on connect-through port

13.4 OSPF Configuration

13.4.1 OSPF overview

OSPF (open shortest path first) is a kind of inner gateway protocol, developed by OSPF work group from Internet Engineering Task Force. This protocol is designed for IP network, which receives outer routing information. All kinds of OSPF messages are encapsulated directly in IP, relays not on other protocols (like TCP, UDP). OSPF supports message validation.

OSPF routing protocol is a kind of link state routing protocol, work on a Autonomous System, which means a group of network that exchange routing information using the uniform routing strategy or routing protocol. In this AS, all the OSPF routers maintain a link state database that describes the topology structure of the whole autonomous system. The link state bulletin in the database describes the state information of corresponding link in the routing domain, like its available interfaces and reachable neighbor routers. Using flooding, the router can broadcast the information to the whole autonomous system.

All the routers run the same algorithm, and establish each other's shortest path tree according to the link state. The shortest path tree gives the shortest route from the router to each destination address in its AS.

OSPF allows several network aggregate to a region, and the structure of the region is invisible to other parts of AS. Using this information hiding, much routing communication can be saved. Beside, because the routing inside the region is decided only by the topology structure of its own, so the region can be protected from the fault routing data. OSPF allows configuring several regions in one AS, but when several regions exist, there must be one backbone region (ID: 0), so that all the regions keep logical connectivity.

OSPF running process:

1. When OSPF protocol is started on router active port, other routers in the same network send out HELLO packets, if there exist two or more routers in all kinds of network that allows multi-addresses visit, 'Designed Router' and 'Backup Designed Router' must be selected in the network. The designed router sees to broadcasting network link state. This concept helps reduce the neighbor relationship number between each switch in the multi-addresses visit network. When the two routers that share the same data link fulfill some designed parameters from the HELLO packets they received, they will become neighbor.

2. The neighbor relationship forms between the routers that exchange routing information.

3. Send LSA among all the routers that have neighbor relationship. LSA describes all the information on router linking, port and link state. These links can reach to STUB network, other OSPF routers, other area's network and outer network (the network that learns routing from another routing process, or the network outside AS). Because there is different types of link state information, OSPF defines several LSA types.

4. HELLO is used to keep the activity state between the neighbors. If the network topology is static, and there are no other activities that raise LSA, it will be sent every 30 minutes.

13.4.2 Configure OSPF

ISCOM obeys OSPFv2, and supports the following features:

- ➢ Stub region – supports stub region concept;
- ➢ Certification – supports plain text and MD5 certification among the neighbor routers in the same region;
- ➢ Router port parameter configuration – on OSPF port the following parameters can be configured: port output cost, re-sending LSA interval, port transmission delay, router priority, hello time interval, dead time interval, certification, certification key word;
- ➢ Virtual-link – virtual link is supported;
- ➢ Not-so-stubby-area (NSSA) – RFC 1587;

One of OSPF features is that, the coordination among many inside-the-domain routers, domain edge routers (connected with many regions) and AS edge router is needed. Without any configuration, the state of the router based on OSPF and visiting server is default parameter value, no validation and the port belongs not to any region. If some configuration parameters have been modified, all the switches' configuration must keep the same.

13.4.2.1 Default OSPF configuration

Function	Default value
OSPF routing protocol	Disable
Designed network RIP protocol	Disable
OSPF interface parameter	Cost: 1 Hello interval: 10s Priority: 1 Retransmit interval: 5s Transmit delay: 1s Dead interval：4 times hello interval Authentication type: none Authentication password: empty MD5 key: empty
OSPF region parameter	Default cost: 1 Range: disable. Stub: no definition NSSA: no definition

	No definition area ID and Router ID
	Hello interval: 10s
	Retransmit interval: 5s
Virtual-link	Transmit delay: 1s
	Dead interval: 4 times hello interval
	Authentication type: none
	Authentication password: empty
	MD5 key: empty

13.4.2.2 Enable OSPF

Use **router ospf** to enable OSPF protocol. Enabling OSPF protocol is the precondition of all the other OSPF configuration tasks. In global configuration mode, type the following commands:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**router ospf**	Enable OSPF

Use **no router ospf** to disable OSPF protocol.

13.4.2.3 Enable the designed network OSPF protocol and appoint region ID

All the ports of the switches that is running OSPF need to be configured into the same region, if there exist several regions in the autonomous system, BackBone (region ID is 0) must be configured.

In OSPF routing protocol configuration mode, use **network** to enable the port that belongs to the command designed network, create a region and add the port to the region. If there is no port that belongs to the command designed network, use the command and the system will create region for only. Specific operations are as follows:

Step	Command	Description
1	**config**	Enter global configuration
2	**router ospf**	Enable OSPF, and turn to protocol configuration mode
3	**network** *network-number netmask* **area** *area-id*	Enable the port that is running OSPF, and define the port region ID

13.4.2.4 Configure OSPF interface parameter

ISCOM allows configure-man change some configuration parameters, but to all the routers that connect to the same network, some specific parameters must be kept the same. These parameters includes: hello-interval, dead-interval, authentication mode and password. If these parameters had been configured in one of the routers in the network, the other routers' configuration must be kept the same with the first one, or the routers will lose connection.

In interface configuration mode, follow the steps below to configure port parameters:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** *ifNum*	Turn to three-layer interface configuration mode
3 (optical)	**ip ospf cost** *cost*	Configure transmission cost for the port
4 (optical)	**ip ospf dead-interval** *seconds*	Configure neighbor dead time interval, that is if there is no HELLO message received from a neighbor in the time interval, then the node will take it as losing connection with the neighbor
5 (optical)	**ip ospf hello-interval** *seconds*	Configure the time interval of sending HELL message
6 (optical)	**ip ospf priority** *priority*	Configure router priority, which is used for DR/DBR polling.
7 (optical)	**ip ospf retransmit-interval** *seconds*	Configure the time interval of port re-sending link state broadcast, the unit is second.
8 (optical)	**ip ospf transmit-delay** *seconds*	Configure the delay value of port transmitting link state broadcast.
9 (optical)	**ip ospf authentication-type** *{simple-password/ message-digest/none}*	Configure port authentication mode.
10 (optical)	**ip ospf authentication-password** *string*	Configure port authentication mode to simple password authentication.
11 (optical)	**ip ospf message-digest-key** *keyid* **md5** *key*	Configure port MD5 authentication

Notice: By default dead-interval is four times of hello-interval, when hello-interval is modified, dead-interval will be modified automatically with four times relationship. But if only dead-interval is modified, hello-interval will not be changed.

13.4.2.5 Configure OSPF region parameters

Configure-man can configure stub region, NSSA region, ABR to stub or the cost of NSSA region default router, aggregate region routing.

Stub region is a region that the outer routing information of the router will not flood to, which decreases the size of link state database, and saves the resource cost of each router processing outer routing information inside the region. The Area Border Router that connects to stub region must use summary-LSAs to proclaim a default link to stub region, these default routing flood in stub region. To decrease more LSA, you can install **no-summary** on stub region border router to configure stub region to totally stubby region, totally stubby region stops not only autonomous system outer routing information flooding but also all summary-LSAs flooding, except summary-LSAs by default.

NSSA (Not-So-Stubby area) is region that does not accept any routing information outside autonomous system, except the routing information sent with LSA TYPE 7. You can also install **no-summary** on border routers of NSSA region, so that the NSSA region stops not only the routing information flood outside LSA TYPE 7 but also all the summary-LSAs flood, except summary-LSAs by default.

Area default-cost command is used only in ABR that is connected to stub or NSSA region. The command configures the cost from ABR to stub/NSSA region default routing.

Border region router can be region centralized or aggregation router. Single aggregation routing uses ABR for other regions' broadcasting, so that routing information can be reduced at region border. Outside the region, each address range will aggregate a routing broadcasting, so that routing table can be reduced. Command parameter means if aggregation routing will be broadcasted.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**router ospf**	Enable OSPF, and turn to protocol configuration mode
3 (optical)	**area** *area-id* **stub** [**no-summary**]	Configure the region to stub region
4 (optical)	**area** *area-id* **nssa** [**no-summary**]	Configure the region to NSSA region
5 (optical)	**area** *area-id* **default-cost** *cost*	Configure the default routing cost from ABR to stub or NSSA region
6 (optical)	**area** *area-id* **range** *ip-address mask* [{**advertise|not-advertise**}]	Aggregate the designed region to designed network routing, if there is **advise** in the command, then a type 3, aggregated LSA affiche aggregation routing will form. If **not-advertise** exists in the command, then it will not form.

Notice: Only when both routers are in the same stub region can they form neighbor relationship, if two routers are within the same network, but one is in stub region while the other one is not, then the two router can not form neighbor relationship, nor can they exchange link state information.

13.4.2.6 Establish/configure virtual link

Virtual link is used to restore or enhance backbone connection, which can be configured between the two ABR in the same region and each of which has a port. Because backbone region must keep logical connection, so if the two nodes in the backbone region have no region routing, or if there is backbone region logical abruption, virtual link must be configured to keep the backbone connection. What's else, by configuring a virtual link from not-backbone region to backbone region, the redundancy rate of backbone region can be enhanced to raise its connection.

Virtual link is marked by the opposite side router ID, the region that provides routing for virtual link is Transmit Area, it is needed to designate Transmit Area when configuring virtual link. A virtual link will be enabled when router finds out its virtual neighbor routing, which can be seen as a unnumbered port to port link in backbone region. So you can configure virtual port parameter.

Virtual link configuration is in OSPF routing protocol configuration mode

Step	Command	Description
1	**config**	Enter global configuration mode
2	**router ospf**	Enable OSPF and turn to protocol configuration mode
3 (optical)	**area** *area-id* **virtual-link** *router-id* [**hello-interval** *hello-interval*]	Create and configure virtual link

[**retransmit-interval** *retransmit-interval*]	
[**transmit-delay** *transmit-delay*] [**dead-interval** *dead-interval*]	
[**authentication-type** {*simple-password* | *message-digest* |*none*}]	
[**authentication-key** *authentication-key*]	
[**message-digest-key** *message-digest-key* **md5** *md5*]	

Notice: Virtual link can not be configured to cross stub region, and it must be configured between two ABR. It will change from state DOWN to up before it finds out ABR routing.

13.4.3 Monitoring and maintenance

Use **show** to show some special data, it helps watching OSPF running state, and handling the running problem. In privileged mode run the commands below:

Command	Description
show ip route	Show routing table
show ip protocol	Show routing protocol and port routing protocol configuration
show ip ospf	Show OSPF collective information
show ip ospf database	Show link state information bank
show ip ospf interface	Show port information in designed port mode
show ip ospf neighbor [*router-id*]	Show neighbor information
show ip ospf virtual-link	Show virtual link information

1. Show OSPF main information

For example: RAISECOM# **show ip ospf**

OSPF region

Region ID	port number	SPF running times	region type
1	*2*	*180*	*neither Stub nor NSSA*
2	*1*	*35*	*neither Stub nor NSSA*
3	*1*	*11*	*Stub*
4	*1*	*25*	*NSSA*

2. Show all the OSPF region link state database information

For example: Raisecom# **show ip ospf database**

Router ID 20.0.0.1

Region: 1

LSA type	Link state ID	Affiche router	Time	Serious number	Checksum

LSA type	Link state ID	Affiche router	time	serious number	Checksum
1	10.0.0.1	10.0.0.1	481	0x80000007	0x86C0
1	13.0.0.2	13.0.0.2	743	0x80000002	0x61AD
3	10.0.0.0	10.0.0.1	732	0x8000000B	0xF63F
3	13.0.0.0	10.0.0.1	2103	0x80000002	0xE359
3	172.22.0.0	13.0.0.2	743	0x80000002	0x4249

Region: 2

LSA type	Link state ID	Affiche router	time	serious number	Checksum
1	10.0.0.1	10.0.0.1	936	0x800000011	0x49F1
1	10.0.0.2	10.0.0.2	538	0x80000008	0x6B86
2	10.0.0.2	10.0.0.2	538	0x80000003	0x7593
3	13.0.0.0	10.0.0.2	923	0x80000001	0x42CD
3	12.0.0.0	10.0.0.2	880	0x80000001	0xEA30
3	172.22.0.0	10.0.0.2	738	0x80000001	0x2831

13.4.4 Typical configuration example

The following are some OSPF configuration examples:

- ➢ OSPF router configuration with different identities.
- ➢ Virtual link configuration;

Example 1: OSPF router configuration with different identities.

1) Topology figure, as is shown in 4-1

Figure 4-1 shows the network figure of a OSPF configuration example. You can see that there exists several OSPF regions and router, inner router, affiche border router with several identities.

2) Configuration explanation

OSPF basic configuration needs 3 necessary steps:

- ➢ Confirm which region each router port is bind to.
- ➢ Use **router ospf** to start OSPF protocol.
- ➢ Use **network** to add the designated port to specific region and run OSPF protocol.

Notice: **area** areaid **stub no-summary** can be configured on stub region border router for only. **area** areaid **nssa no-summary** can be configured on nssa region border router for only.

3) Configuration step

Configure router A – inner router

! Configure interface 0

Raisecom(config)# **interface ip** *0*

Raisecom (config-ip)# **ip address** *192.108.1.1 255.255.255.0 1*

! Configure OSPF protocol

Raisecom (config)#**router ospf**

Raisecom (config-router-ospf)#**network** *192.108.1.0 0.0.0.255* **area** *1*

Configure router B – inner router

! Configure interface 6

Raisecom (config)#**interface ip** *6*

Raisecom(config-if)#**ip address** *192.108.1.2 255.255.255.0 2*

! Configure OSPF

Raisecom (config)#**router ospf**

Raisecom (config-router-ospf)#**network** *192.108.1.0 0.0.0.255* **area** *1*
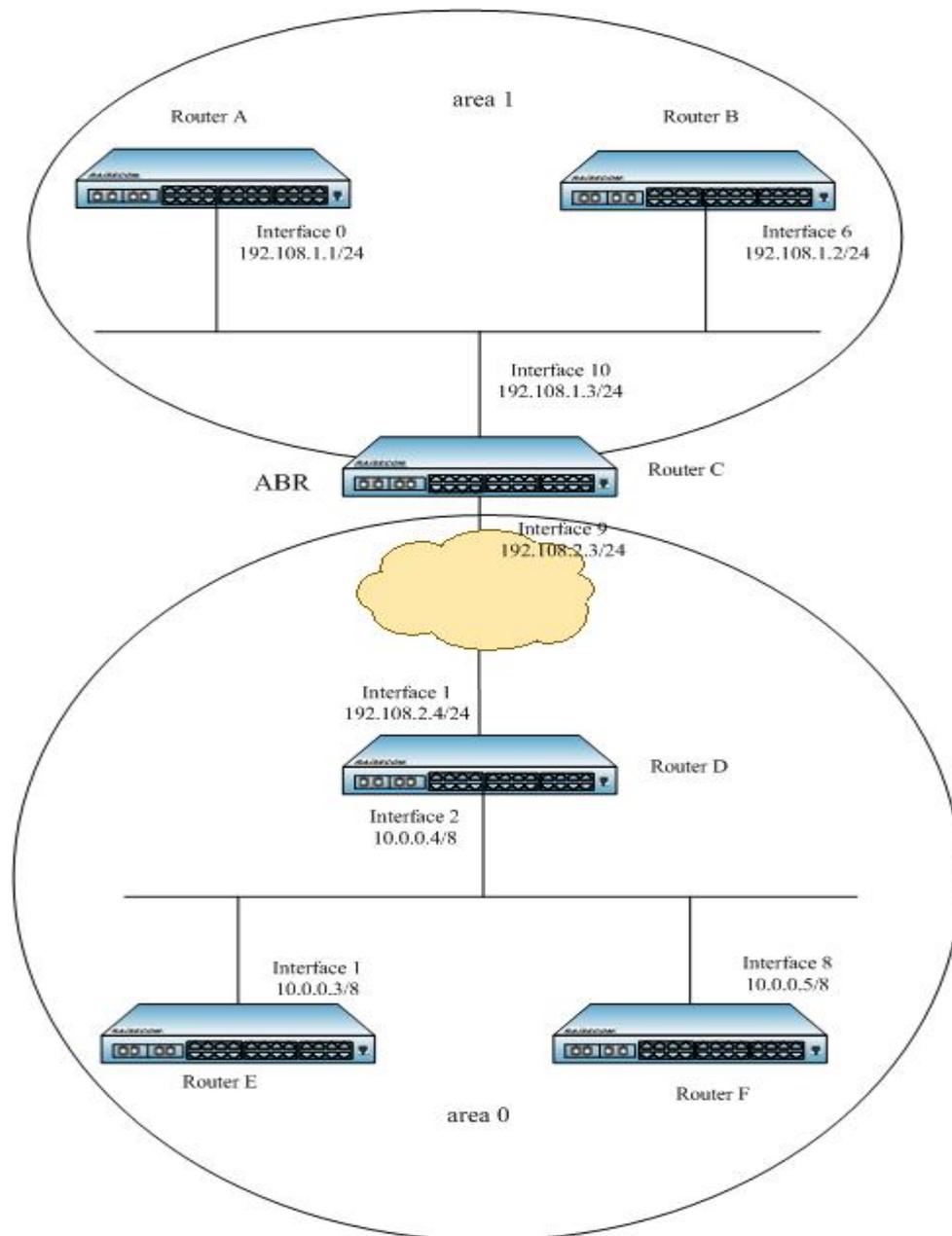
Fig 4-1 OSPF different identities router configuration

Configure router C – ABR

! Configure interface 10

Raisecom (config)#**interface ip** *10*

Raisecom (config-if)#**ip address** *192.108.1.3 255.255.255.0 1*

! Configure OSPF protocol

Raisecom (config)#**router ospf**

Raisecom (config-router-ospf)#**network** *192.108.1.0 0.0.0.255* **area** *1*

! Configure interface 9

Raisecom (config)#**interface ip** *9*

Raisecom (config-if)#**ip address** *192.108.2.3 255.255.255.0 1*

! Configure OSPF protocol

Raisecom (config)#**router ospf**

Raisecom (config-router-ospf)#**network** *192.108.2.0 0.0.0.255*   **area** *0*

Configure router D – inner router

! Configure interface 1

Raisecom (config)#**interface ip** *1*

Raisecom (config-if)#**ip address** *192.108.2.4 255.255.255.0 1*

! Configure OSPF protocol

Raisecom (config)#**router ospf**

Raisecom (config-router-ospf)#**network** *192.108.2.0 0.0.0.255* **area** *0*

! Configure interface 2

Raisecom (config)#**interface ip** *2*

Raisecom (config-if)#**ip address** *10.0.0.4 255.0.0.0 2*

! Configure OSPF protocol

Raisecom (config)#**router ospf**

Raisecom (config-router-ospf)#**network** *10.0.0.0 0.255.255.255* **area** *0*

Configure router E – inner router

! Configure interface 1

Raisecom (config)#**interface ip** *1*

Raisecom (config-if)#**ip address** *10.0.0.3 255.0.0.0 1*

! Configure OSPF protocol

Raisecom (config)#**router ospf**

Raisecom (config-router-ospf)#**network** *10.0.0.0 0.255.255.255* **area** *0*

Configure router F – inner router

! Configure interface 8

Raisecom (config)#**interface ip** *8*

Raisecom (config-if)#**ip address** *10.0.0.5 255.0.0.0 2*

! Configure OSPF protocol

Raisecom (config)#**router ospf**

Raisecom (config-router-ospf)#**network** *10.0.0.0 0.255.255.255* **area** *0*

Example 2: virtual link configuration

1) Topology figure 4-2

2) Configuration instructure

Figure 4-2 shows a network topology structure that is not so well designed. Suppose there is no Router E in the figure, and there are four routers in the backbone region, suppose the link between A and B has been broken, then it will lead to backbone region abruption. Router C and D can not communicate with each other. If the two router are the only ABR of each other's region, it will lead to routing information block between the regions. The best way for this problem is to add a redundant actual physical link, but to some reason, the physical link between C and D can not be established. Then we can take a compromising way: establish a virtual link between A and B to keep the connection. Notice, you'd better not use virtual link in actual working, because the existence of virtual link show the shortage of the network design, and the network is not in good state.

3) Configuration steps:
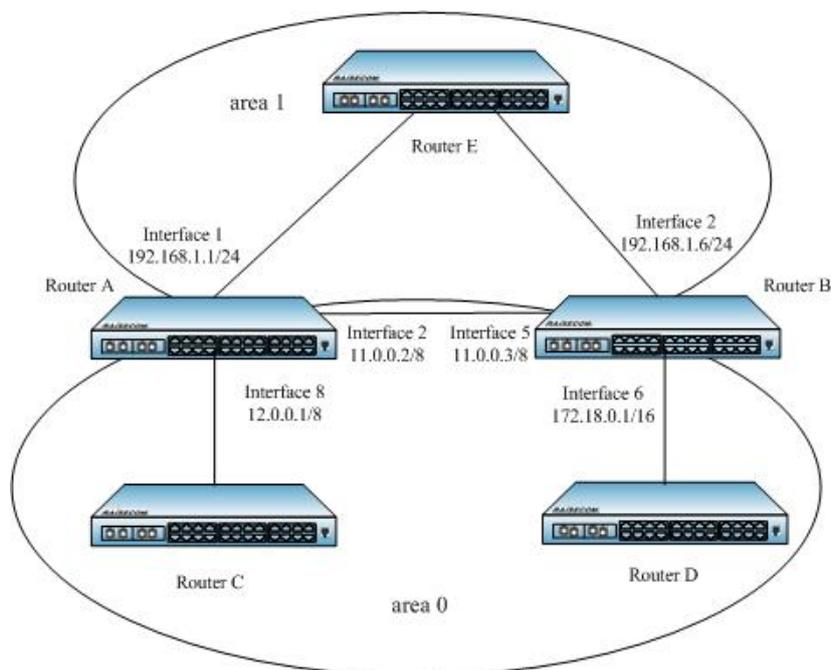
Fig 4-2 Virtual link configuration

Configure router A

! Configure interface 1

Raisecom(config)#**interface ip** *1*

Raisecom(config-if)#**ip address** *192.168.1.1 255.255.255.0 1*

! Configure interface 8

Raisecom(config)#**interface ip** *8*

Raisecom(config-if)#**ip address** *12.0.0.1 255.0.0.0 4*

! Configure interface 2

Raisecom(config)#**interface ip** *2*

Raisecom(config-if)#**ip address** *11.0.0.2 255.0.0.0 3*

! Configure OSPF protocol

Raisecom(config)#**router ospf**

Raisecom(config-router-ospf)#**network** *12.0.0.0 0.255.255.255* **area** *0*

Raisecom(config-router-ospf)#**network** *11.0.0.0 0.255.255.255* **area** *0*

Raisecom(config-router-ospf)# **network** *192.168.1.0 0.0.0.255* **area** *1*

Raisecom(config-router-ospf)# **area** *1* **virtual-link** *192.168.1.6*

Configure router B

! Configure interface 5

Raisecom(config)#**interface ip** *5*

Raisecom(config-if)#**ip address** *11.0.0.3 255.0.0.0 1*

! Configure interface 6

Raisecom(config)#**interface ip** *6*

Raisecom(config-if)#**ip address** *172.18.0.1 255.255.0.0 4*

! Configure interface 2

Raisecom(config)#**interface ip** *2*

Raisecom(config-if)#**ip address** *192.168.1.6 255.255.255.0 3*

! Configure OSPF protocol

Raisecom(config)#**router ospf**

Raisecom(config-router-ospf)#**network** *11.0.0.0 0.255.255.255* **area** *0*

Raisecom(config-router-ospf)#**network** *172.18.0.0 0.0.255.255* **area** *0*

Raisecom(config-router-ospf)# **network** *192.168.1.0 0.0.0.255* **area** *1*

Raisecom(config-router-ospf)#**area** *1* **virtual-link** *192.168.1.1*

13.4.5　OSPF trouble shooting

> ➢　Fault case 1:

Two straight connecting router have all been configured OSPF protocol on the same network port, but the protocol can not work well, and the two sides can not reach FULL state.

Trouble shooting:

Step 1: check out if all the ports have correct address and mask.

Step 2: check out if each port has been configured to the correct region, the two ports needs to be in the same region.

Step 3: check out if the physical connection and underlayer protocol is running normally. Use **ping** to examine it, if local router can not ping the opposite router through, it means that the physical connection and underlayer protocol have problems. In addition, if the port is POS type, check out if PPP protocol has been encapsulated, that is to run **encapsulation PPP**.

Step 4: check out if the interface parameter of each router is the same type, which includes hello-interval, dead-interval and authentication type and password.

Step 5: if one area is configured to stub region, then all the routers connected to the region should configure the region to stub region, or the communication can not be established.

➢ Fault 2:

When there are several regions configured in the network, the routing information of each region is incomplete.

Trouble shooting:

When 2 or more regions exists, backbone region (region ID: 0) must be configured to ensure the region connection.

➢ Fault 3:

When virtual link is configured, use **show ip ospf virtual-link** and find that virtual port is not in active state.

Trouble shooting:

Step 1: check out the cross region of virtual link, it can not go through stub region

Step 2: check out ABR routing, if there is not then virtual port can not be in active state.

Chapter 14   Multicast Protocol

14.1 Multicast Overview

14.1.1 The confusion of unicast/broadcast

As Internet develops, on one side the interactive data, voice and video information in the network are becoming more and more, on the other side the rising services like electronic commerce, network meeting, network auction, video on demand and remote education are in gradual rise. These services have new request on information security and payment, which traditional unicast and broadcast can not meet well.

14.1.1.1   Information transmission in unicast

With unicast, the system will establish a single data transmission channel for the user who needs the information, and send a single copy to the user, as is shown below:
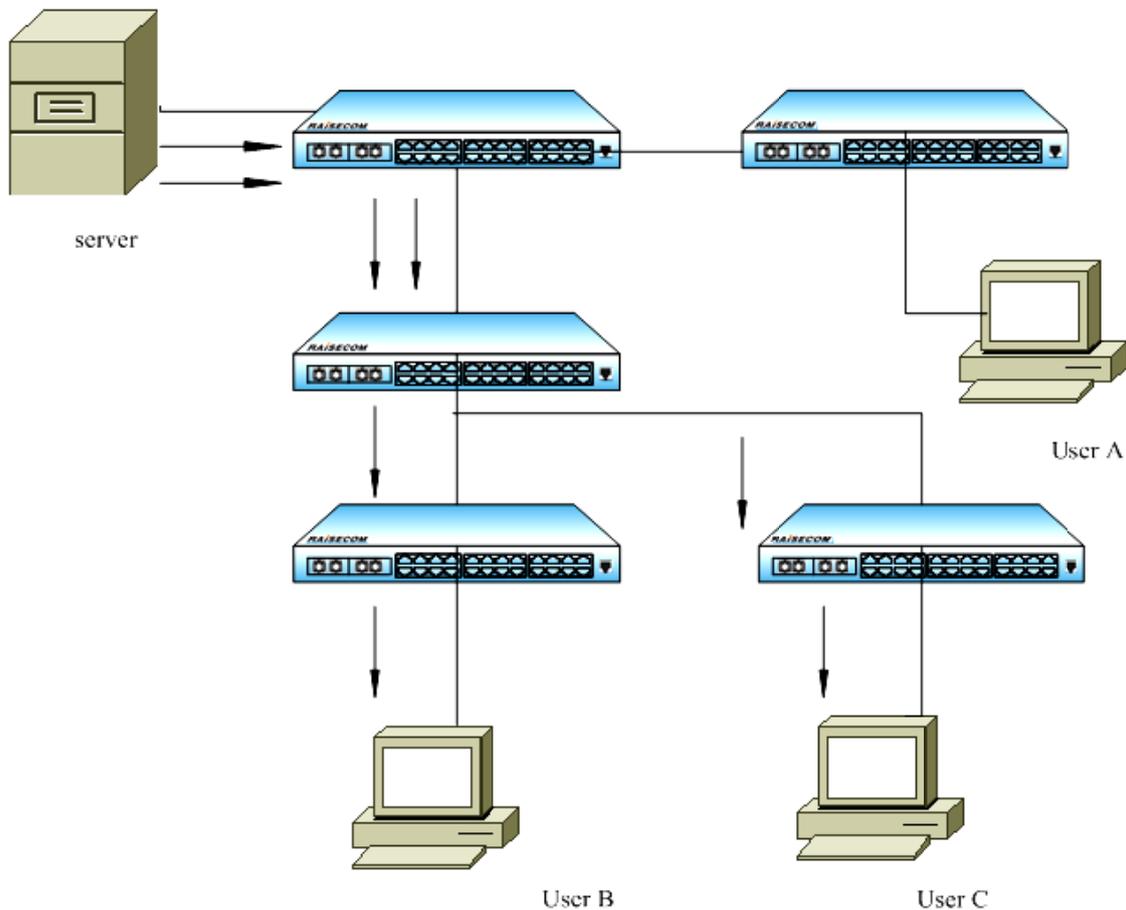
Fig 1-1 unicast transmission

Suppose user B and C need the information, the information source Server will establish transmission channel for user B and C respectively. Because the information capacity transmitted in the network is in proportion to the capacity of users who need the information, when the number of users who need the information is large, there will be several same information stream in the network. Then bandwidth will be

a important bottleneck and unicast goes against sending information in large scale.

14.1.1.2 Transmitting information in broadcasting

Using broadcast, the system will send the information to all the network users, caring not if it is needed, any user can receive the information from broadcasting, as is shown below:
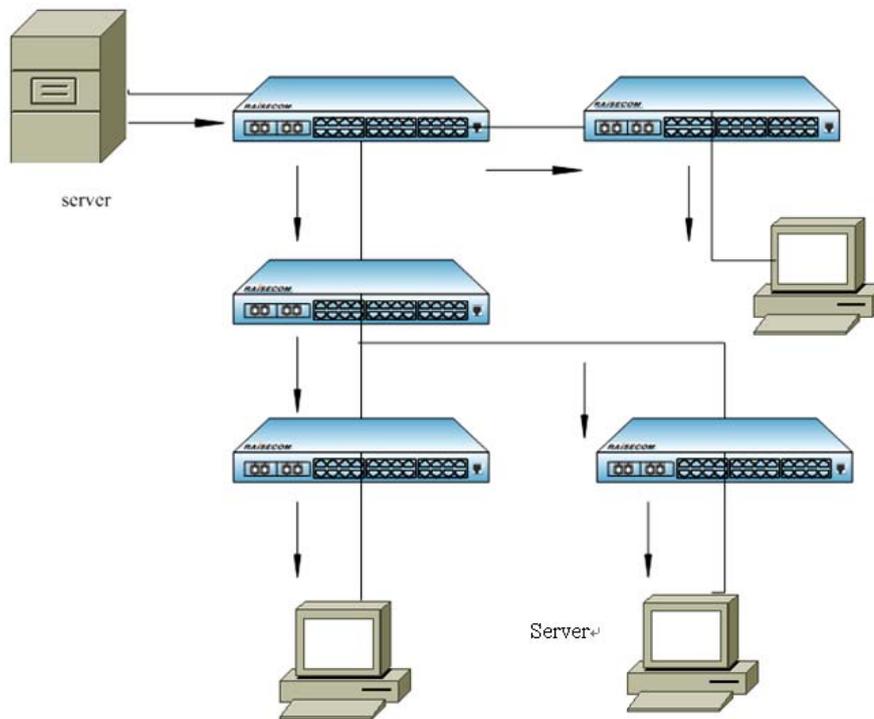
server

Fig 1-2 Information transmission in broadcast

Suppose user B and C need the information, then information source Server will broadcast the information by router, another network user A can also receive the information, which means information security and payment services can not be ensured. On the other side, when there is not so many users who need the information, network resource use ratio will be quite low, which is a great waste of the bandwidth. In summary, unicast suits the network with rare users, while broadcast suit the network with a lot of people. When the number of users who need the information is not so sure, unicast and broadcast are both low in efficiency.

14.1.2   The advantage of multicast

14.3.4.1 Information transmission in multicast

The appearance of multicast handles the problem in time. When some users in the network need specific information, multicast source send out information only once, and the information sent out will be copied and sent out in the crossing as far as possible, as is shown below:
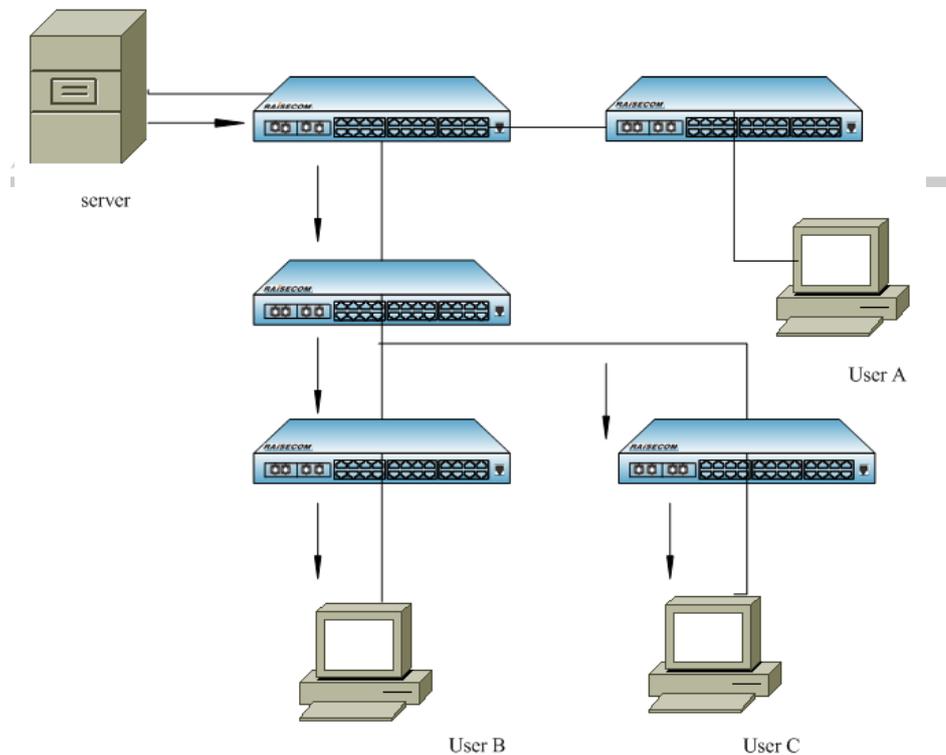
Fig 1-3 Information transmission in multicast

Suppose user B and C need the information, to send the information successfully to the user who really needs it, it is needed to form B, C into a receiver combination, then each switch in the network form its own multicast transmission table according to IGMP message, at last the information will be transmitted accurately to receiver B, C who need it really. In multicast information sender is called 'multicast source', but some information receiver call it the 'multicast group' of the information. The receiver member who joins the same multicast group can be located in any place in the network, that is to say, there is no domain limit with 'multicast group'. It should be noted that multicast source does not have to belong to multicast group, it send data to multicast group and don't have to be receiver itself. There can be several sources sending out messages to one multicast group.

14.3.4.2 Information transmission in multicast

The advantage of multicast is:

Increase the efficiency and decrease the network traffic, ease the load of the server and CPU;

Optimize the performance and decrease the redundant traffic;

Distributed application makes multi-point use possible.

14.2 IGMP Snooping Configuration

This chapter is mainly about how to configure and maintain IGMP Snooping, including:

- ✧ About IGMP Snooping
- ✧ Configuration task list
- ✧ Monitoring and maintenance
- ✧ Typical application
- ✧ Trouble shooting

14.2.1 About IGMP Snooping protocol

IGMP Snooping, unlike ISO module, has no clear concept module, which takes the upper-layer protocol data information as the bottom-layer working consideration factor. In the transmission of multicast, IGMP Snooping confines data flooding to all the ports, but transmits information only to the multicast member ports, which helps saving the bandwidth.

IGMP snooping allows LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure MAC multicast groups by using the **ip igmp snooping static** command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings. Raisecom series switches supports 1024 two-layer multicast transmission table item, and support IGMPv1 and IGMPv2 version.

14.2.2 IGMP snooping configuration

This part is about how to configure and maintain IGMP Snooping on switch, including:

- ✧ Enable and disable IGMP Snooping
- ✧ IGMP Snooping aging time
- ✧ Multicast Router port configuration
- ✧ Configuring immediate-leave function
- ✧ Manually configure multicast MAC address table.

14.2.2.1 Default IGMP Snooping configuration

Function	Default value
IGMP SNOOPING starting	On
IGMP SNOOPING out-time	300 秒
Configure the router time	Do not configure
MVR mode	Compatible
Quit immediately	Disabled
Multicast stable transmission table	Not configured

14.2.2.2 IGMP Snooping enable and disable

IGMP snooping is disabled on the switch by default. If IGMP snooping is globally enabled/disabled, all the VLAN will enable or disable IGMP snooping function. The following commands are used to enable IP

IGMP Snooping:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip igmp snooping**	Enable IGMP Snooping
3	**exit**	Exit to privilege mode
4	**show ip igmp snooping**	Show configuration situation

Use **no ip igmp-snooping** command to disable IP IGMP Snooping.

This command is used to globally disable IGMP snooping function. In order to disable IP IGMP snooping function on particular VLAN, use the following commands under VLAN configuration mode.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**vlan** *vlan-id*	Enter VLAN configuration mode
3	**no ip igmp snooping**	Disable the IGMP snooping function for this VLAN.
4	**exit**	Exit to global configuration mode
5	**exit**	Exit to privileged EXEC mode
6	**show ip igmp snooping vlan** *vlan-id*	Show VLAN configuration information

In order to enable IGMP snooping function on the VLAN, use **ip igmp snooping** in VLAN configuration mode.

If IGMP snooping is disabled globally, IGMP snooping function can not be enabled on particular VLAN.

If user needs to enable or disable IGMP Snooping function on several VLANs, use **ip igmp-snooping vlan** command in global configuration mode according to the following table:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip igmp snooping vlan 1-100**	Enable IGMP snooping function on VLAN1-100
3	**exit**	Exit to privileged user mode
4	**show ip igmp snooping**	Show IGMP Snooping configuration information

Use **no ip igmp snooping vlan** command to disable IGMP snooping function on several VLAN at a time.

In order to check whether the configuration is correct or not, use show command:

Raisecom#**show ip igmp snooping**

IGMP snooping: Enable

IGMP snooping aging time: 300s

IGMP snooping active VLAN: 1,2

IGMP snooping immediate-leave active VLAN: --

Raisecom#**show ip igmp snooping vlan** *2*

> *IGMP snooping: Enable*
>
> *IGMP snooping aging time: 300s*
>
> *IGMP snooping on VLAN 2: Enable.*
>
> *IGMP snooping immediate-leave on VLAN 2: Disable.*

14.2.2.3 IGMP snooping aging time configuration

If switch does detect IGMP Snooping Join or Query message within a period, the subscriber may have left already without sending any leaving message, so the switch needs to be deleted the multicast MAC address from the address table. The default aging time is 300 seconds. Configuration steps are showed as follows:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**ip igmp snooping timeout** *timeout*	Set IGMP overtime.
3	**exit**	Exit to privilege EXEC mode
4	**show ip igmp snooping**	Show IGMP Snooping configuration information

The range of aging time is 30 seconds to 3600 seconds, in order to recover default value, use following command: **no ip igmp snooping timeout**

Example:

Raisecom#**config**

SCOM2826(config)# **ip igmp snooping timeout** *1200*

ISCOM2826(config)#**exit**

Raisecom#**show ip igmp snooping**

> *GMP snooping: Enable*
>
> *IGMP snooping aging time: 3000s*
>
> *IGMP snooping active VLAN: 1, 2*
>
> *IGMP snooping immediate-leave active VLAN: 1*

14.2.2.4 Router port configuration

The Multicast Router port can be assigned by dynamically address learning (through IGMP request message), or manually configured (that is to say, multicast report and leave message of downlink hosts can be forwarded to multicast router port). The manual configuration steps of multicast router port are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip igmp snooping mrouter vlan** *<1-4094>* **port** *<1-26>*	Configure router port

3	exit	Exit to privileged EXEC mode
4	**show ip igmp snooping mrouter**	Show Multicast Router port configuration information

Use following command to delete configured Multicast Router port: no ip igmp snooping mrouter vlan 1 port 2.

Configuration example:

ISCOM2826#**config**

ISCOM2826(config)#**ip igmp snooping mrouter vlan** *1* **port** *2*

ISCOM2826(config)#**exit**

ISCOM2826#**show ip igmp snooping mrouter**

Ip Address   Port   Vlan   Age   Type

224.0.0.0/8   2   1   --   USER

14.2.2.5 Immediate-leave function configuration:

When you enable IGMP Immediate-Leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port.

The settings are as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**vlan 1**	Enter VLAN configuration mode
3	**ip igmp snooping immediate-leave**	Set immediate-leave function on the VLAN.
4	**exit**	Exit to global configuration mode.
5	**exit**	Exit to privilege EXEC mode.
6	**show ip igmp snooping**	Show IGMP Snooping configuration information

In VLAN configuration mode, use **no ip igmp snooping immediate-leave** command to restore default setting:

Configuration example:

ISCOM2826#**config**

ISCOM2826 (config)#**vlan 1**

ISCOM2826 (config-vlan)# **ip igmp snooping immediate-leave**

ISCOM2826 (config-vlan)#**exit**

ISCOM2826 (config)#**exit**

ISCOM2826#**show ip igmp snooping vlan** *1*

IGMP snooping: Enable

IGMP snooping aging time: 300s

IGMP snooping on VLAN 1: Enable.

IGMP snooping immediate-leave on VLAN 1: Enable.

In order to configure the immediate-leave function in multiple VLAN, use following commands:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**ip igmp snooping vlan** *vlanlist* **immediate-leave**	Set immediate-leave function on the VLAN.
3	**exit**	Exit to privileged EXEC mode.
4	**show ip igmp snooping**	Show IGMP Snooping configuration information

In order to restore default settings, use following command: **no ip igmp snooping vlan** *vlanlist* **immediate-leave**

Example:

iscom2016#**config**

iscom2016(config)# **ip igmp snooping vlan** *1-10* **immediate-leave**

iscom2016(config)#**exit**

iscom2016#**show ip igmp snooping**

> *igmp snooping is globally Enabled*
>
> *igmp snooping aging time is 1200(s)*
>
> *IGMP snooping active vlan: 1*
>
> *IGMP snooping immediate-leave active vlan:1-10*

14.2.2.6 Stable multicast transmission table configuration

Usually a port joins multicast router through the IGMP report message from the host. For maintenance, you can add a port to the multicast group manually.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mac-address-table static multicast** *mac-addr* **vlan** vlanid **port-list** *portlist*	Add the port to the multicast group
3	**exit**	Exit to privilege user mode
4	**show mac-address-table multicast**	Show multicast MAC address information

The MAC address is the multicast MAC address, and the format is HHHH.HHHH.HHHH. For example, multicast IP address 224.8.8.8 is mapped to multicast MAC address 0100. 5e08.0808; the range of the port is from 1 to 26. In order to delete the port from multicast group manually, use command **no mac-address-table static multicast** mac-addr **vlan** vlanid **port-list** portlist.

Configuration example:

Raisecom#**config**

ISCOM2826(config)# **mac-address-table static multicast** *0100.5e08.0808* **vlan** *2* **port-list** *1-6*

ISCOM2826(config)#**exit**

ISCOM2826# **show mac-address-table multicast**

Multicast filter mode: Forward-all

Vlan   Group Address   Ports[Static](Hardware)

---

2   0100.5E08.0808   1-6[1-6](1-6)

14.2.3 Monitoring and maintenance

Use show command to check switch IGMP snooping running and configuration status:

Step	Command	Description
1	**show ip igmp snooping** [**vlan** *vlan-id*]	Show IGMP snooping configuration information in all the VLAN or designated VLAN of the switch.
2	**show ip igmp snooping multicast** [**vlan** *vlan-id*]	Show multicast router port information (dynamically learned or manually configured) of all the VLAN or a designated VLAN.
3	**show mac-address-table multicast** [**vlan** *vlan-id*] [**count**]	Show all the multicast MAC address; *Count*: indicates the total number of multicast MAC address

Use s**how ip igmp snooping** command to check configuration information, for example the timer, VLAN configuration information.

Show IGMP Snooping configuration information:

Raisecom# **show ip igmp snooping**

IGMP snooping: Enable

IGMP snooping aging time: 300s

IGMP snooping active VLAN: 1, 2

IGMP snooping immediate-leave active VLAN: 1

Use **show ip igmp snooping vlan** *vlanid* command to show the IGMP snooping information in a particular VLAN. If you do not specify VLAN, all the VLAN information will be displayed, that is all the existent and active VLAN.

Show igmp-snooping multicast router information:

Raisecom# **show ip igmp snooping mrouter**

Ip Address   Port   Vlan Age   Type

--

224.0.0.0/8   4   3   --   USER

Raisecom#show mac-address-table multicast

Multicast filter mode: Forward-all

Vlan   Group Address   Ports[Static](Hardware)

--

2   0100.5E08.0808   1-6[1-6](1-6)

14.2.4 Typical configuration example

1) Configuration instruction:

To realize the switch IGMP Snooping function, it is needed to start IGMP Snooping on the switch (by default it's on). The router port (physical port 1) on the switch connects to the router, while other not-router ports connect to users' PC.

2) Typical network structure figure
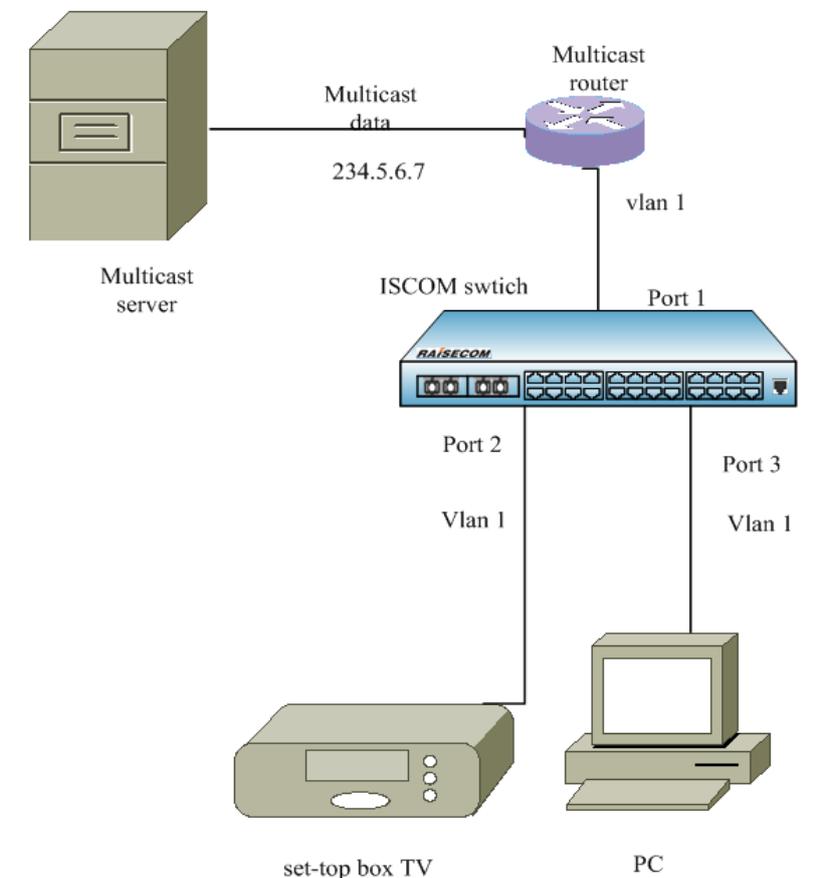
Fig 2-1 Typical IGMP Snooping network structure

3) Configuration command

By default IGMP Snooping function is on, and it will be started to the existed VLAN port. For fig 2-1, use **ip igmp snooping mrouter vlan 1 port 1** to configure the router port on the switch.

14.2.5 IGMP snooping trouble shooting

1.   If multicast router port has not been specified, all the IGMP reports will be transmitted to the port directly connected to the router;

2.   If it is failed to add port to a multicast group manually, the reason may be incorrect multicast MAC address format or the maximum layer 2 multicast router table (255) has been achieved;

3.   If it is failed to delete the port from multicast group manually, the possible reason may be incorrect multicast MAC address format or MAC address/VLAN/port are not existent in multicast router.

14.3   MVR Configuration

This chapter is mainly about how to configure and maintain MVR and IGMP filtration on the switch, including:

- ✧   MVR overview
- ✧   MVR proxy principle introduction
- ✧   IGMP filtration overview
- ✧   MVR configuration
- ✧   MVR monitoring and maintenance
- ✧   MVR proxy configuration
- ✧   MVR proxy monitoring and maintance
- ✧   IGMP filtration configuration
- ✧   IGMP filtration monitoring and maintainance
- ✧   Typical configuration example
- ✧   MVR and IGMP filtration trouble shooting

14.3.1 MVR principle

Multicast VLAN registration is applied as traffic multicast in the network of service provider, such as TV programme ordering. MVR allows subscriber on the port to order or cancel the multicast traffic in VLAN, allows data traffic sharing for different VLANs. There are two MVR aims:

1. By using simple configurations, use can transmit multicast among different VLANs safely and effectively;

2. Support multicast group joining and leaving dynamically;

The operation manner of MVR is similar to that of IGMP snooping. These two functions can be enabled simultaneously. MVR only processes the joining and leaving of configured multicast groups, the other multicast groups are managed by IGMP snooping. The difference between these two is that: with IGMP snooping, the multicast traffic can be transmitted within only one VLAN, while with MVR the multicast traffic can be transmitted within different VLANs.

There are two operation modes:

1. Compatible mode: all multicast data received at the source port (port connected with multicast router) will be forwarded to the other ports, no matter whether these source ports have members to join in or not. Simultaneously, multicast data are only forwarded to those receiving ports (ports connected with subscribers) which are specified to have already joined in the MVR group, the joining can be in the form of IGMP report or MVR static configuration. IGMP report will not be forwarded to the source port of switch. Therefore, the switch dose not support source port joining dynamically. Under this mode, multicast router should be configured as forwarding all multicast data to the source port, since switch will not send IGMP joining information to the router.

2.   Dynamic mode: Received multicast data are only forwarded to those ports which have member to join (source port or receiving port), the joining can be in the form of IGMP report information or MVR static configurations. All received IGMP information is forwarded to the source port of the switch. This method could save much bandwidth.

MVR are operative only on Layer-2. It dose not work on Layer-3. One switch can configure only one multicast VLAN, support 256 multicast groups at most.

14.3.2 MVR proxy principle

MVR proxy provides a complete solution for the multicast operation of two-layer equipments through proxy mechanism. The two-layer network equipments that support MVR proxy take the role of Server on user side, and query user information periodically, and it take the role of Client on the web side, sending the current user's information to the network when needed. This will not only stop the two-layer multicast from flooding, but also help acquiring and controlling user information, at the same time it can help reduce the web side protocol messages and the network load. MVR proxy establish multicast table by holding up the IGMP messages between user and router, the up-link port of Proxy equipment takes the role of host, while down-link port takes the role of router.

14.3.3 IGMP filtration introduction

Administrator needs to limit the multicast users under some circumstances, such as to allow which ports to receive multicast on a switch, which ports to reject multicast data. Use can realize this kind of control on the port by configuring IGMP profile. One IGMP profile includes one or multiple multicast groups, and permit/deny items to access these groups. If one "deny" type IGMP profile is applied to the port, when the port receives IGMP joining information of this group, it will drop and do not allow receiving multicast data from this group. IGMP profile can be applied to dynamic multicast group, not suitable for static group.

In addition, the maximum multicast group can be configured on port.

14.3.4 MVR configuration

This part is about how to configure MVR on the switch, including:

   ✧   Default MVR configuration
   ✧   Global MVR configuration
   ✧   Configure MVR port information

14.3.4.1 Default MVR configuration

Attributes	Default configuration
MVR enable/disable	disabled
Multicast address	Not configured
MVR timeout	600 seconds
Multicast VLAN	1

MVR mode	compatible
Port MVR enable/disable	disabled
Port default configuration	Non MVR（neither source port, nor receiving port）
Intermediate leave	disabled

The steps below should be followed:

➢ Receiving port can be only ACCESS port, but cannot be TRUNK port. Receiving port can belong to different VLANs, but cannot belong to multicast VLAN;
➢ The maximum MVR multicast address is 256;
➢ Since ISCOM28 series switches support Layer-2 multicast, which means multiple IP multicast addresses correspond to one MAC multicast address, MVR multicast address is not allowed using repetitive names during configuration.
➢ MVR and IGMP snooping can coexist；
➢ Source port should be in the multicast VLAN;

14.3.4.2 Global MVR configuration

Under the default situation, MVR is disabled. User can carry out the commands below to enable MVR under global configuration mode. Multicast VLAN, multicast address, operation modes can be configured as well. If MVR has not been enabled yet, it is allowed to configure MVR. Once MVR is enabled, these configurations will take effect at once.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mvr enable**	Enable MVR
3	**mvr group** *ip -address* [*count*]	Configure IP multicast address, if the parameter count is specified, you can configure a consecutive MVR group addresses (the range for count is from 1 to 256, 1 by default)
4	**mvr timeout** *timeout*	optional，MVR multicast entity timeout, unit is second, range is from 60 to 36000, 600 seconds by deflault.
5	**mvr vlan** *vlanid*	Optional, to specify the VLANs for receiving multicast, all source ports should belong to this VLAN. Range is from 1 to 5094. 1 by default.
6	**mvr mode** *{dynamic|compatible}*	Optional, MVR operation modes: dynamic: Dynamic mode compatible: Compatible mode
7	**exit**	Back to privileged EXEC mode
8	**show mvr**	Show MVR configuration
9	**show mvr members**	Show MVR group address

To disable MVR, carry out command **mvr disable** under global configuration mode. To set the other configurations back to default status, you can use the command **no mvr {mode | group** *ip-address* **| timeout | vlan}.**

Command **mvr group** *ip –address* indicates which multicast traffic can be received. If this parameter is not specified, all traffics will be received.

The example below shows how to enable MVR, how to configure multicast address, timeout and multicast

vlan:

raisecom(config)# **mvr enable**

raisecom (config)# **mvr group** *234.5.6.7*

raisecom (config)# **mvr timeout** *180*

raisecom (config)# **mvr vlan** *22*

raisecom (config)# **mvr mode dynamic**

To check if the configurations are correct, use command **show**:

Raisecom#**show mvr**

> *MVR Running: Enable*
>
> *MVR Multicast VLAN: 22*
>
> *MVR Max Multicast Groups: 256*
>
> *MVR Current Multicast Groups: 1*
>
> *MVR Timeout: 180 (second)*
>
> *MVR Mode: dynamic*

To view MVR group address configurations:

Raisecom#**show mvr members**

> *MVR Group IP   Status   Menbers*
>
> *--*
>
> *234.5.6.7   Inactive   none*

14.3.4.3 MVR port information configuration

Under default situation, ports on switch are neither receiving port, nor source ports. User can configure them under interface configuration mode:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mvr**	enable MVR
3	**interface port 3**	Enter interface configuration mode
4	**mvr**	Enable interface MVR
5	**mvr type** *{source/receiver}*	Mvr type configuration: *source*: uplink port can be configured as souce port for receiving multicast data, this port cannot be connect directly to subscribers, all source ports should belong to multicast VLAN. *receiver*: configured as to connect subscribers straightforward, cannot belong to multicast VLAN.
6	**mvr vlan** *vlanid* **group** *ip-address*	Optional, set the port to join multicast group statically. Under compatible mode, this command can applied to receiving port, and can be applied to source port or receiving port dynamically.

7	**mvr immediate**	Enable automatic leaving function onthis port, this command can be only applied on receiving port
8	**exit**	Back to global configuration mode
9	**exit**	Back to privileged EXEC mode
10	**show mvr**	Show MVR configuration status
11	**show mvr port** [*portid*]	Show port mvr configuration information
12	**show mvr port** [*portid*] **members**	Show port member information

To set port MVR configuration back to default status, you can use command **no mvr** [**type** | **immediate** | **vlan** *vlan-id* **group**]. Use command **no mvr vlan** *vlan-id* **group** to delete all static multicast group, you can specify a multicast address if you want to delete only one group. The example below shows how to configure port 3 as MVR receiving port, and how to enable intermediate leaving function and how to join into the static multicast group:

Raisecom#**config**

Raisecom(config)#**inter port** *3*

Raisecom(config-port)#**mvr**

Raisecom(config-port)#**mvr type receiver**

Raisecom(config-port)#**mvr immediate**

Raisecom(config-port)#**mvr vlan** 1 **group** *234.5.6.7*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

To check if the configurations are correct, use command **show**:

Raisecom#**show mvr port** *3*

   Running: Enable

   Type: Receiver

   Status: Inactive/down

   Immediate Leave: Enable

Raisecom#**show mvr port** *3* **members**

   MVR Group IP   Type   Status

   --

   234.5.6.7   static   Inactive

14.3.5 MVR monitoring and maintaining

You can use some "show" commands to view the MVR running status and configurations for the switch in which way you can achieve a better monitor and maintenance:

Command, mode	Commands below need to run under ENABLE mode

show mvr	Show MVR global configuration information
show mvr members	show MVR group information
show mvr port [*portid* **]**	show MVR port configuration information
show mvr port *portid* **members**	Show MVR static or dynamic group information

Show MVR global configuration information

Raisecom#**show mvr**

> *MVR Running: Enable*
>
> *MVR Multicast VLAN: 1*
>
> *MVR Max Multicast Groups: 256*
>
> *MVR Current Multicast Groups: 0*
>
> *MVR Timeout: 600 (second)*
>
> *MVR Mode: Compatible*

Show MVR group information

Raisecom#**show mvr members**

> *MVR Group IP   Status   Menbers*
>
> *--*
>
> *234.5.6.7   Active   1*
>
> *234.5.6.8   Active   1*
>
> *234.5.6.9   Inactive   None*
>
> *234.5.6.10   Inactive   None*

Show MVR port configuration information

Raisecom#**show mvr port**

> *Port   Running   Type   Status   Immediate Leave*
>
> *---*
>
> *1   Enable   Receiver   Inactive/down Enable*
>
> *2   Disable   Non-MVR   Inactive/down Disable*
>
> *3   Disable   Non-MVR   Inactive/down Disable*
>
> *4   Disable   Non-MVR   Inactive/down Disable*
>
> *5   Disable   Non-MVR   Inactive/down Disable*
>
> *6   Disable   Non-MVR   Inactive/down Disable*
>
> *7   Disable   Non-MVR   Inactive/Up   Disable*
>
> *......*
>
> *25   Disable   Non-MVR   Inactive/down Disable*
>
> *26   Disable   Non-MVR   Inactive/down Disable*

To show designated port information:

Raisecom#**show mvr port** *1*

> *Running: Enable*
>
> *Type: Receiver*
>
> *Status: Inactive/down*
>
> *Immediate Leave: Enable*

Show MVR port group information

Raisecom#**show mvr port** *1* **members**

> *MVR Group IP   Type   Status*
>
> *---*
>
> *234.5.6.7   static   Inactive*
>
> *234.5.6.8   static   Inactive*

14.3.6 Configure MVR Proxy

This part is about how to configure MVR proxy on the switch, including:

- ✧   Default MVR proxy configuration
- ✧   Configure MVR proxy
- ✧   MVR proxy monitoring and maintaining

14.3.6.1 Default MVR proxy configuration

Feature	State
Message compress function	disable
Querier function	disable
MVR proxy source IP address	Use the IP address of IP port 0, if IP port 0 is not configured, use 0.0.0.0
Query time interval	60s
The maximum responding time of sending query message	10s
The last member sending query interval	1s

14.3.6.2 MVR Proxy configuration

By default, MVR proxy is off on the switch. In global configuration mode use the following commands to activate MVR proxy configuration. You can also set source IP address, query time interval, the maximum responding time of sending query message, the last member sending query interval. If MVR proxy is not started, configuring MVR proxy is allowed, and once MVR proxy is started, these configurations will take

effect immediately.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mvr proxy**	Start MVR proxy function. When it is started, MVR message compress function and MVR querier function will be started at the same time.
3	**mvr proxy suppression**	Start message compress function
4	**mvr proxy querier**	Start querier function
5	**mvr proxy source-ip** *A.B.C.D*	Optical, the given MVR proxy packet source IP address. If not configured use the IP address of IP port 0, if IP port 0 is not configured, use 0.0.0.0
6	**mvr proxy query-interval** *seconds*	Optical, set the querier query time interval. Default value is 60s, range is 10-65535
7	**mvr proxy query-max-response-time** *seconds*	Optical, set the maximum responding time of query message. Default value is 10s, range is 1-25
8	**mvr proxy last-member-query** *seconds*	Optical, configure the last member sending query interval, default value is 1s, range is 1-25

To stop MVR proxy, in global configuration mode run command **no mvr proxy** to disable message compress and querier function. In global configuration mode use **no mvr proxy suppression** and **no mvr proxy querier** to disable message compress and querier function respectively. To restore other configurations to default value, use **no mvr proxy {source-ip | query-interval | query-max-response-time | mvr proxy last-member-query}.**

The following example shows how to start MVR proxy, set the source IP to 192.168.0.1, query interval 100s, query message maximum responding time 20s, the last member sending query interval 5s.

Raisecom (config)# **mvr proxy**

Raisecom (config)# **mvr proxy source-ip** *192.168.0.1*

Raisecom (config)# **mvr proxy query-interval** *100*

Raisecom (config)# **mvr proxy query-max-response-time** *20*

Raisecom (config)# **mvr proxy last-member-query** *5*

Use command **show** to examine if the configuration is correct:

Raisecom # **show mvr proxy**

Mvr proxy suppression status:	*enable*
Mvr proxy querier status:	*enable*
Mvr proxy source ip:	*192.168.0.1*
Mvr proxy version：	*V2*
Mvr query interval(s):	*100*
Query Response Interval(s):	*20*
Last Member Query Interval(s):	*5*
Next IGMP general query(s):	*5*

14.3.7 MVR Proxy monitoring and maintenance

Use the commands below to show MVR proxy configuration and port MVR static.

Command	Description
show mvr proxy	Show MVR proxy configuration
show mvr port [*portid*] statistics	Show port MVR static
clear mvr port [*portid*] statistics	Clear port static information

Show MVR proxy configuration:

Raisecom # **show mvr proxy**

Mvr proxy suppression status:　　　　　　　　*enable*

Mvr proxy querier status:　　　　　　　　*enable*

Mvr proxy source ip:　　　　　　*192.168.0.1*

Mvr proxy version：　　　　　　*V2*

Mvr query interval(s):　　　　　*100*

Query Response Interval(s):　　　　　*20*

Last Member Query Interval(s):　　　　*5*

Next IGMP general query(s):　　　　　　*5*

Show port MVR static

Raisecom # **show mvr port statistics**

Port 1:

Received query packets: 10

Received report packets: 10

Received leave packets: 10

Drop query packets: 10

Drop report packets: 10

Drop leave packets: 10

Last replace new multicast address: 224.1.1.1

Last replace old multicast address: 224.2.2.2

Total replace count: 5

Port 2:

Received query packets: 10

Received report packets: 10

Received leave packets: 10

Drop query packets: 10

Drop report packets: 10

Drop leave packets: 10

Last replace new multicast address: 224.1.1.1

Last replace old multicast address: 224.2.2.2

Total replace count: 5

……

14.3.8 IGMP filter configuration

This part is about how to configure IGMP filter on the switch, including:

- ✧ Default IGMP filter configuration
- ✧ IGMP profile configuration
- ✧ Use IGMP profile

14.3.8.1 Default IGMP filter configuration

Feature	state
IGMP filter enable/disable	Enabled
Port application	No application
Maximum group	No limit
Maximum group action	Reject
IGMP profile	Not defined
IGMP profile action	reject

14.3.8.2 IGMP profile configuration

Use command **ip igmp profile** under global configuration mode, you can create IGMP profile and enter profile configuration mode. Parameters such as range, actions and etc. can be configured under this mode.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip igmp profile** *profile-number*	Create profile and enter profile configuration mode, series number of profile is from 1 to 65535.
3	**permit | deny**	Optional, actions configuration including permit or deny multicast group access, the default status is deny.
4	**range** *start-ip* [*end-ip*]	IP multicast address or address range

		configurations. If inputting address range, the starting address, blanks and ending address should be within the group address.
5	**exit**	Back to global configuration mode
6	**exit**	Back to privileged EXEC mode
8	**show ip igmp profile** [*profile-number*]	Show IGMP profile configuration information

To delete profile, carry out **no ip igmp profile** under global configuration mode. To delete a multicast address of profile, use command **no range** *start-ip*.

The example below shows how to create profile 1 and configure single multicast address:

raisecom(config)# **ip igmp profile** *1*

raisecom (config-profile)# **range** *234.5.6.7*

raisecom (config-profile)# **range** *234.5.6.9*

raisecom (config-profile)# **permit**

raisecom (config-profile)#**exit**

raisecom (config)#**exit**

To check if the configurations are correct, use command show:

Raisecom#**show ip igmp profile** *1*

> *IGMP profile 1*
>
> *permit*
>
> *range 234.5.6.7*
>
> *range 234.5.6.9*

14.3.8.3 Appling IGMP filter under interface

Use command **ip igmp filter** under interface configuration mode to apply the created IGMP profile on a specified port. One IGMP profile can be applied to multiple ports, but one port can have only one IGMP profile.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** *1*	Enter interface mode
3	**ip igmp filter** *profile-number*	Apply IGMP profile on the port
4	**ip igmp max-groups** *group-number*	Set the maximum number of the groups that is allowed for entry
5	**ip igmp max-groups action** *{deny	replace}*	The action taken when the group number on the port exceeds the maximum group number
6	**exit**	Return to global configuration mode

7	**exit**	Return to privileged EXEC mode
8	**show ip igmp filter port** [*portid*]	Show the IGMP profile applied on the port

To cancel applying IGMP profile, use command **no ip igmp filter** under interface configuration mode. If no IGMP profile is applied to port, no result will be shown.

The example below shows how to apply IGMP profile 1:

raisecom(config)# **interface port** *1*

raisecom (config-port)# **ip igmp filter** *1*

raisecom (config-port)#**exit**

raisecom (config)#**exit**

To check if the configurations are correct, use command **show**:

Raisecom#**show ip igmp filter port**

Port	*Filter*	*Max Groups*	*Current Groups*	*Action*
1	*1*	*20*	*0*	*Deny*
2	*0*	*20*	*0*	*Deny*
3	*0*	*0*	*0*	*Deny*
......				
25	*0*	*0*	*0*	*Deny*
26	*0*	*0*	*0*	*Deny*

To view port 1 information:

Raisecom#**show ip igmp filter port** *1*

IGMP Filter: 1

Max Groups: 20

Current groups: 0

Action: Deny

14.3.8.4 Appling IGMP filter under VLAN

By default, there is no IGMP filter applying rules under VLAN, no maximum group limit, the maximum group action is deny. Follow the steps below in global configuration mode to configure the applied filter rules under VLAN, maximum group limit and maximum action.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip igmp filter profile vlan vlanlist**	Specify the defined filter rules on VLAN. The

		applied filter rule number should have been created, or the configuration fails. Vlanlist range is 1-4094.
3	**ip igmp max-group** **max-group vlan vlanlist**	Set the maximum group number on specified VLAN. The configured maximum group number must be no larger than the maximum group number that the equipment supports
4	**ip igmp max-group action** *{deny|replace}* **vlan vlanlist**	Configure the maximum group action the specified VLAN, default value is 'deny'.
5	**exit**	Return to privileged EXEC mode
6	**show ip igmp filter vlan** *[vlanid]*	Show the configured filter information under VLAN.
7	**config**	Enter global configuration mode
8	**ip igmp filter profile vlan vlanlist**	Specify the defined filter rules on VLAN. The applied filter rule number should have been created, or the configuration fails. Vlanlist range is 1-4094.

Use **no ip igmp filter vlan** *vlanlist* to delete the configured filter rules under VLAN, use **no ip igmp max-group vlan** *vlanlist* to delete the configured maximum group limit under VLAN.

The following example shows how to apply filter rules under VLAN and configure the maximum group limit and maximum group action:

Raisecom (config)# **ip igmp filter** *1* **vlan** *1*

Raisecom (config)# **ip igmp max-group** *10* **vlan** *1*

Raisecom (config)# **ip igmp max-group action replace vlan** *1*

Use the command **show** to examine if the configuration is correct

Raisecom # **show ip igmp filter vlan** *1*

VLAN   Filter   Max Groups   Current Groups   Action

--

1   1   10   0   Replace

14.3.9 IGMP filter monitoring and maintenance

Use some **show** commands to show the switch IGMP filter running state and configuration state for monitoring and maintenance. Use the following **show** commands to do IGMP filter monitoring and maintenance:

Command	Description
show ip igmp filter	Show IGMP filter global configuration information
show ip igmp profile [*profile-number*]	Show IGMP profile information
show ip igmp filter port [*portid*]	Show IGMP filter port configuration information
show ip igmp filter vlan [*vlanid*]	Show the IGMP filter rules configuration under specified VLAN. When vlanid is not specified, show the configuration state of VLAN that have been configured filter rules.

14.3.10 Typical configuration example

14.3.10.1 MVR typical configuration example

PC or TV set-top box can receive multicast traffics, one or multiple PC or televisions can connect to a receiving port called subscriber. When selecting scheduled programs, set-top or PC sends IGMP report information to join a group. If IGMP report matches to the configured multicast addresses on the switch, the CPU on the switch will modify the multicast switch table in the hardware, and add this port to the multicast VLAN group. When the source port receives the multicast traffic, it will send the traffic to the receiving ports according to the multicast forwarding table in the hardware.

When switching channels or shutting down the TV, the set-top box or PC will send IGMP leaving information, then the switch will forward this information to the multicast router, the router will send IGMP query information, if there is no other member in this group, the switch will delete this port from the group.

If enabling immediate leaving function on the receiving port, port will leave the group faster. If the immediate leaving function is not enabled yet, when the receiving port receives IGMP leaving information, the switch will forward router's IGMP query information and wait IGMP member report. If no report is received within the maximum query time, the member will be deleted from the group. If enabling the immediate leaving function, port member will be deleted as soon as it receives IGMP leaving information. This feature is normally used in the situation that one port is connected to only one user.

Multicast traffic will not be transmitted in all VLANs, but only need to be transmitted in multicast VLAN. Use can save much bandwidth in this way.
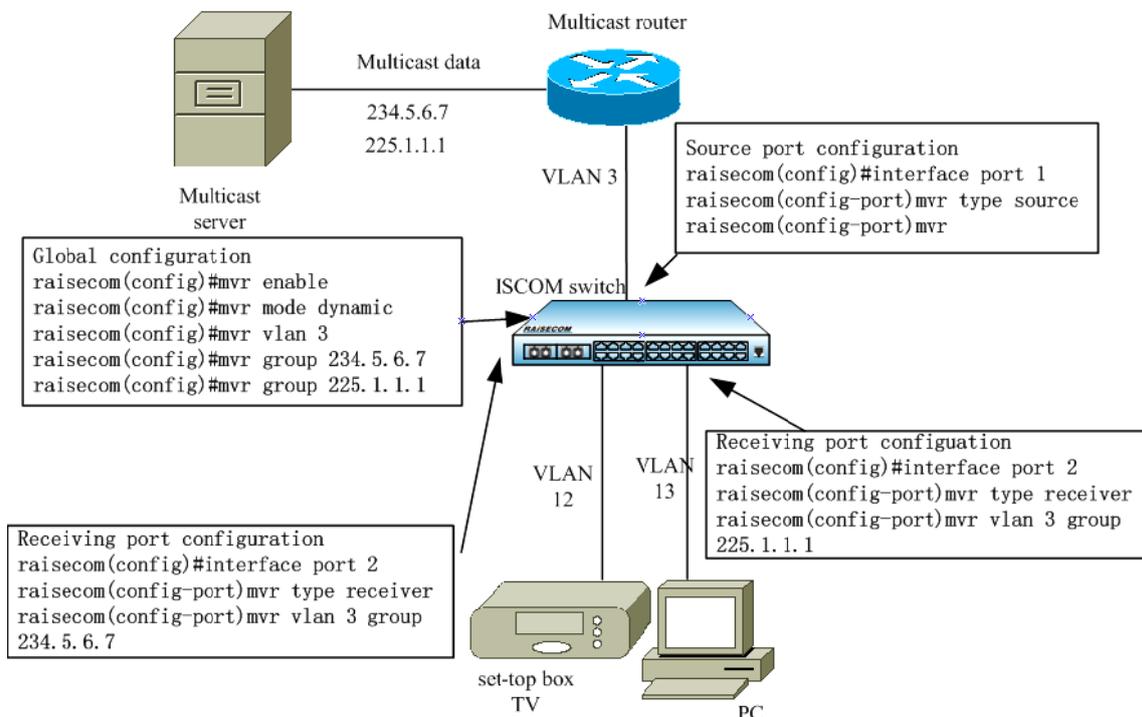
Fig 3-1 MVR application topology

14.3.10.2 MVR proxy typical configuration example

Enable MVR proxy on ISCOM switch: configure port 1 to source port, port 2 and 3 to receive port. In the figure below, when PC and set-top box join the same multicast group, the switch will receive two IGMP report messages, and send only one IGMP report message to the multicast router. The IGMP query message sent from multicast router will no longer transmit to downstream, but send IGMP query message by the switch periodically.
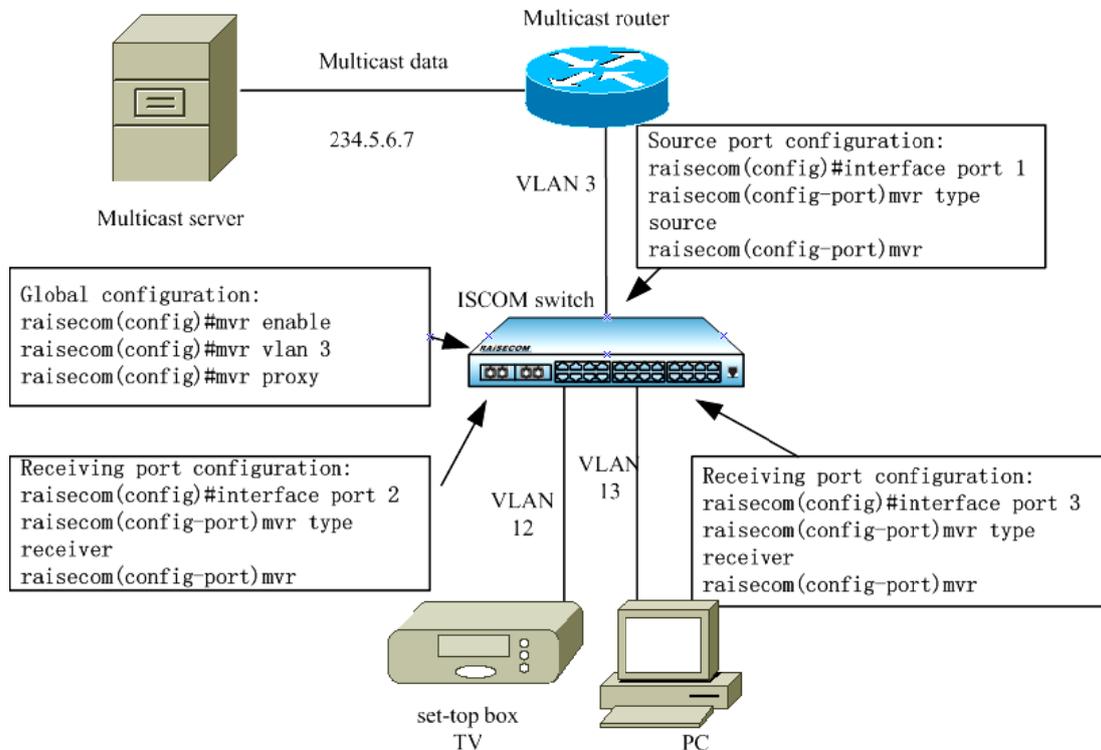
Fig 3-2 MVR proxy application topology

14.3.10.3 IGMP filter under VLAN typical configuration example

Enable IGMP filter on the switch, establish filter rule profile 1, and set address range from 234.5.6.7 to 234.5.6.10, the action is set to allow. According to the IGMP filter rule under VLAN 12, PC and set-to box can both enter the multicast group 234.5.6.7, PC can join the multicast group 234.5.6.11 while set-top box can not. According to the maximum group limit of VLAN 12, after set-top box enter 234.5.6.7, if it enter 234.5.6.8, it will quit from the multicast group 234.5.6.7 before.
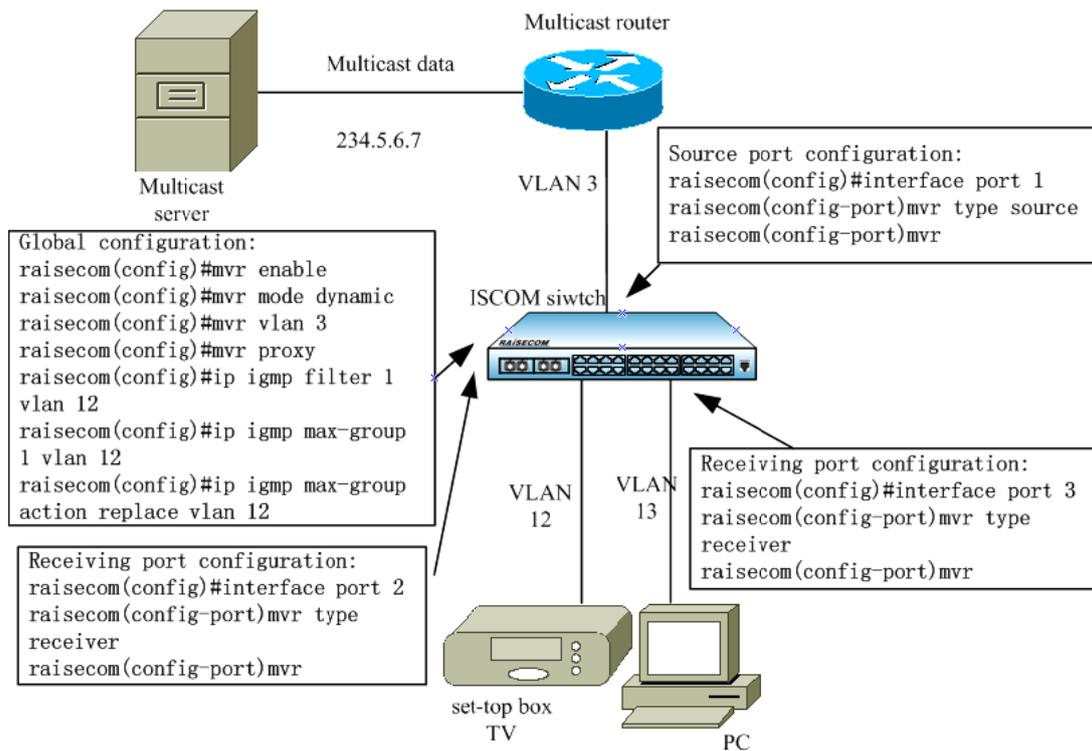
Fig 3-3 the IGMP filter application topology under VLAN

14.3.10.4   The IGMP filter under port typical configuration example

Enable IGMP filter on the switch, establish filter rule profile 1, and set address range from 234.5.6.7 to 234.5.6.10, the action is set to allow. According to the IGMP filter rule under port 2, PC and set-to box can both enter the multicast group 234.5.6.7, PC can join the multicast group 234.5.6.11 while set-top box can not. According to the maximum group limit of port 2, after set-top box enter 234.5.6.7, if it enter 234.5.6.8, it will quit from the multicast group 234.5.6.7 before.
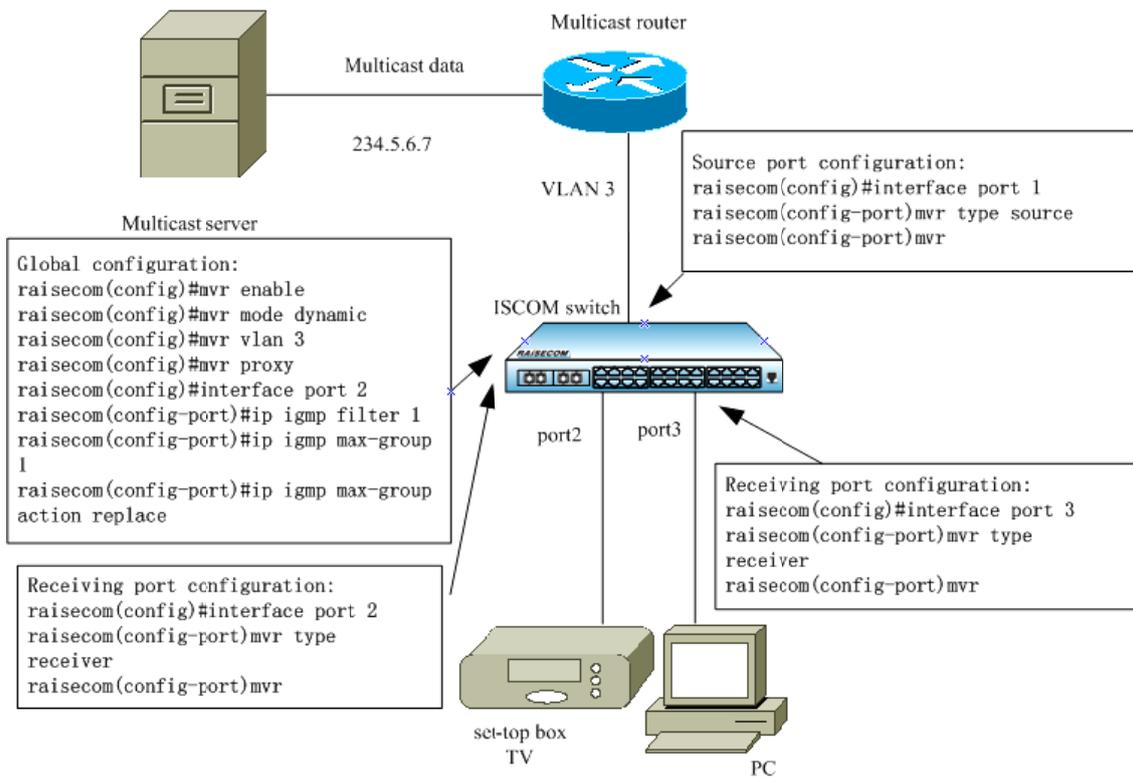
Fig 3-4 the IGMP filter application topology under port

14.3.11 MVR, MVR Proxy and IGMP filter trouble shooting

1. When configuring source port, it is not within multicast VLAN;

2. When configuring receive port, it is in multicast VLAN;

3. When configuring MVR group, the group addresses conflict because several IP multicast addresses suit one MAC multicast address;

4. When configuring stable group on the port, the address is not within MVR range;

5. In MVR compatible mode, configure stable multicast on source port.

Chapter 15   VLAN

15.1 VLAN Principle

15.1.1 IEEE802.1Q VLAN

VLAN stands for virtual LAN (virtual Local Area Networks). In terms of functions, VLAN has the same characteristics with LAN. However, VLAN members are not restricted by physical locations. For instance, the users connected to the same switch can belong to different VLANs. The broadcast domain and multicast domain are both in reference to VLAN member, multicast, broadcast and unicast will not flood to other VLANs. Different VLANs can communicate with each other only via Layer-3 switch or router. The features above offer much convenience for network management, user can allocate VLANs based on functions in the network so as to promote the network bandwidth utility and security. A typical VLAN network topology is shown below:
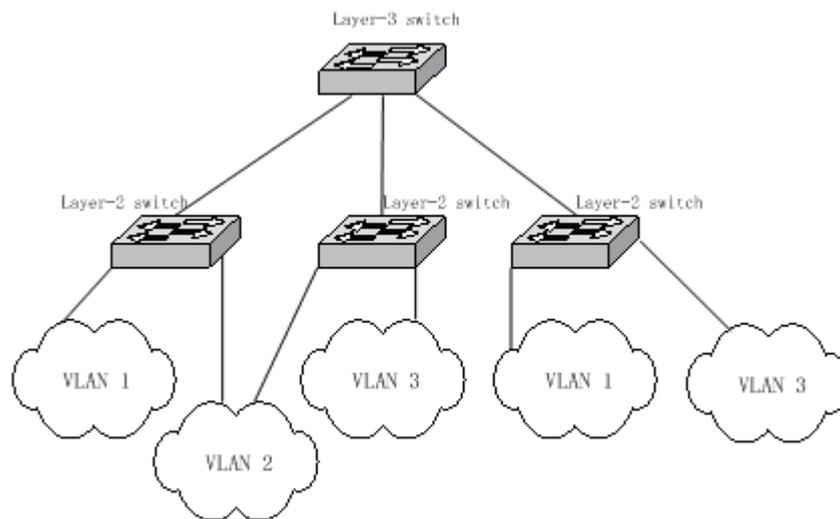
VLAN, a protocol to handle the Ethernet problems from broadcasting and safety, is added VLAN port based on Ethernet frame, divides users into smaller working group using VLAN ID and limits the two-layer visit between users within different working groups. Each working group is a virtual LAN.

In 1999 IEEE issues the 802.1Q protocol standard draft for VLAN realization project. As the criterion of VLAN, it encapsulates VLAN ID in the frame header, so that the VLAN information can be kept when a frame is crossing different equipments. The switches of different producers can be under unified management and cross switches if only they support 802.1Q VLAN.

15.1.2 VLAN Mapping interview

VLAN Mapping can modify VLAN Tag in the message, and supports the following two mapping relationships:

1: 1VLAN Mapping: change the VLAN ID in VLAN Tag taken by a message into another VLAN ID.

2: 2VLAN Mapping: add out-layer VLAN Tag to the message with one layer VLAN Tag, so that the message can take two layer VLAN Tag.

15.1.3 Q-IN-Q interview

In the framework of IP data network, the switch is used as access equipment, when LAN is used as the

access process, to divide users for user's data safety becomes a serious problem.

Now many producers demands end to end safety recognition, hoping each user can allocated a VLAN, but the problem is that there are only 4096 standard VLAN resources. However, using the innovative Q-in-Q technology, the limit of 4096 VLAN can be broken through in metro Ethernet assembly, which not only extends the ability of creating two-layer network using VLAN, but also realizing metro network two-layer VPN, that is suitable for metro network and WAN services.

Q-in-Q technology is a simple and flexible two-layer VPN technology. Using outer-layer VLAN Tag to encapsulate outer-layer VLAN Tag for user's private network message in carrier's access end, it can let the message carry two-layer VLAN Tag to cross carrier's backbone network (public network). Inner layer VLAN Tag is user private network VLAN Tag, outer layer VLAN Tag is the one that carrier allocates to user. In public network, messages transmit only according to the outer layer VLAN Tag, and the source MAC address table item of the messages is learned and copied to the MAC address table of the VLAN that outer layer Tag is in, while user's private network VLAN Tag will be taken as the messages' data part for transmission.

The basic working principle and method of Q-in-Q: when the data is transmitting in private network it has a private network mark, defined as CVLAN Tag; when entering the backbone network of facilitator, public network VLAN Tag will be added to it, defined as SPVLAN Tag (or Outer tag); when reaching destination private network the SPVLAN Tag of the public network will be deleted to offer user a relatively simple two-layer VPN tunnel. SPVLAN Tag is embedded after Ethernet source MAC address and destination MAC address, which also contains a 12 bits SPVLAN ID that supports 4096 VLAN. SPVLAN CoS domain contains 3 bits, supports 8 priority. In the network based on Q-in-Q, the operator allocates a SPVLAN ID for each VLAN, then maps user's CVLAN ID to these SPVLAN ID. Thus, user's C-VLAN ID can be protected.

15.2 Switch VLAN Function Configuration

15.2.1 VLAN based on port

VLAN division based on port is the most simple and effective way for VLAN division. It defines VLAN member according to the equipment port, and when the given port enters the given VLAN, it can transmit messages from the given VLAN

15.2.1.1 VLAN port mode interview

Port member mode	VLAN member attributes
Access	Under this mode, the port can be allocated to a single VLAN, packet sent from Access port does not have no 802.1Q tag, Access ports within different VLANs cannot communicate with each other.
Hybrid	Under this mode, the port can be allocated to multiple VLANs, you can also determine if packet sent out from Hybrid port carries related 802.1Q tag or not. Meanwhile, you can also classify the non-802.1Q packets that enter the port into different VLANs by setting the Native attribute of the port.
Trunk	Trunk port can be allocated with different VLANs by default, packet forwarded from it carries 802.1Q tag expect for Native VLAN. However, you can limit the packets through which VLAN they are forwarded by using *allowed vlans*

Dot1q-tunnel	TUNNEL port mode can only be designated to one VLAN by user, the data packet transmitted from TUNNEL port do not contain out layer TAG, TUNNEL port of different VLAN can not interflow. The data packet entered from TUNNEL port can be added two layer TAG.
Trunk double-tagging	Configure port to TRUNK mode, and enable the port the ability of recognizing and handling out layer TAG (that is SP VLAN TAG).
Hybrid dot1q-tunnel	Configure the port to HYBRID mode, enable the port the ability of adding outer layer TAG (that is SP VLAN TAG) for the packet entering the port (ignoring the out-layer/inner-layer TAG in the data packet)

15.2.1.2 Default VLAN configuration

Function	Default value
Create stable VLAN	There are default VLAN and cluster VLAN in the system, that is VLAN 1 and VLAN 2, all the ports exists in VLAN 1 in access mode
VLAN name	The default system VLAN (VLAN 1) is 'Default', cluster VLAN name is 'Cluster-Vlan', other stable VLAN name is 'VLAN' adding VLAN ID(four figures number)
Configure the activity state of stable VLAN	The new created stable VLAN activity state is suspend.
Configure the port mode	Access
Configure the VLAN number that is allowed to pass in HYBRID mode	All VLAN
Configure the VLAN number that is allowed to pass in TRUNK mode	VLAN1
Configure Native VLAN for Trunk, Hybrid port	VLAN1
VLAN filtration attribute	Enable
Port protection	The port is not protected port
Transmission port list	All the other ports except its own port
VLAN priority	No priority

15.2.1.3 Configure VLAN Attribute

VLAN attribute configuration includes the VLAN configuration of creation, deletion, name and activity state. The configuration steps are as follows:

Step	Command	Command parameter explain
1	**config**	Enter global configuration mode
2	**create vlan** {2-4094} **(active|suspend) priority** {*0-7*}	Create VLAN and make sure the state: active/suspend 0-7: VLAN priority {2-4094}: VLAN ID

3	**vlan** *<1-4094>*	Create VLAN and enter the configuration mode *<1-4094>* VLAN ID
4	**name** *WORD*	Dominate VLAN *WORD* VLAN name, no longer than 15 characters
5	**state** {**active** | **suspend**}	Configure VLAN state: active/suspend
6	**exit**	Return to global configuration mode
7	**exit**	Return to privileged EXEC mode
8	**show vlan**	Show VLAN configuration

Use **no vlan** *<2-4094>* to delete VLAN.

Notice：

➢ The new created VLAN using VLAN <1-4094> is in suspend state, if user wishes to activate it in the system, the command **state** that would be introduced later is needed to activate VLAN.
➢ By default there are VLAN existed in the system, that is default VLAN (VLAN 1) and cluster VLAN (VLAN 2), all the ports are Access mode belongs to the default VLAN. VLAN priority range is 0-7.
➢ The new created VLAN, has no priority by default, is shown as N/A. VLAN priority range is 0-7.
➢ By default, default VLAN (VLAN 1) name is 'Default', cluster VLAN (VLAN 2) name is 'Cluster-VLAN', other VLAN name is character stream 'VLAN' added four figures VLAN ID. For example, the default VLAN 1 name is 'VLAN0001', the default VLAN 4094 name is 'VLAN4094'.
➢ All the VLAN configuration can no take effect until the VLAN is activiated. When VLAN activity state is suspend, user can still configure the VLAN, like delete/add port, configure VLAN name and so on, the system will keep the configuration, once the VLAN is activated, the configuration will take effect in the system.

15.2.1.4 Configure VLAN priority

By default, when VLAN is created, there is no priority, shown as N/A, the VLAN priority range is 0-7. The configuration steps are as follows:

Step	Command	Command parameter example
1	**config**	Enter global configuration mode
2	**vlan** {*2-4094*} **priority** *<0-7>*	Configure VLAN priority {*2-4094*} VLAN ID *<0-7>* VLAN priority
3	**exit**	Return to privileged EXEC mode
4	**show vlan**	Shown VLAN configuraion

Use **no vlan** {2-4094} **priority** to restore VLAN priority to default state, or VLAN without priority.

15.2.1.5 Configure port VLAN mode

Each mode and the configuration is shown below:

1. Configure port VLAN mode

Port VLAN mode configuration must be done in physical interface configuration mode, the steps are as

follows:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface port** *portid*	Enter the corresponding physical port configuration mode *portid*: port number
3	**switchport mode** *{access |* *hybrid [double-tagging]| trunk* *[double-tagging]| [hybrid]* *dot1q-tunnel}*	Configure port VLAN mode access ACCESS mode, that is port exists in the unique VLAN in the form of UNTAG; hybrid HYBRID mode, port can exist in several VLAN in both UNTAG or TAG mode hybrid double-tagging Configure the port to HYBRID mode, and enable the port the ability of recognizing and handing outer layer Tag (or SP VLAN Tag) hybrid dot1q-tunnel configure the port to HYBRID mode, and enable the port the ability of compulsively adding outer layer Tag (or SP VLAN Tag) for the packets. trunk TRUNK mode, port exists in several VLAN in TAG mode, and exists in Native Vlan in UNTAG mode. trunk double-tagging configure the port to TRUNK mode so that it is able to recognize and handle outer layer Tag (or SP VLAN Tag) dot1q-tunnel TUNNEL mode, the data packet enters from theis port can be added double Tag
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface port** [*port-list*] **switchport**	Show port VLAN attribute configuraion

Use **no switchport mode** to restore port VLAN mode to default value, that is port VLAN mode is Access mode.

2. Configure Access, dot1q-tunnel port Access VLAN, the steps are as follows:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface port** *portid*	Enter physical port configuration mode
3	**switchport access vlan** *<1-4094>*	Configure VLAN that is allowed to pass Hybrid port
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface port** [*port-list*] **switchport**	Show port VLAN attribute configuration

Use **no switchport access vlan** command to restore Access VLAN to default value, or port Access VLAN is VLAN 1.

3. Configure VLAN that is allowed to pass through Hybrid port ,the steps are as follows:

Step	Comamnd	Description
1	**config**	Enter global configuration mode
2	**interface port** <1-26>	Enter the corresponding physical port configuration mode
3	**switchport hybrid allowed vlan { all** | *vlan-list* | **add** *add-vlan-list* | **remove** *remove-vlan-list***}**	Configure the allowed VLANs for the Hybrid port All: allow all vlan vlan-list: allow all VLAN, rewrite the primary configuration Add: add-vlan-list: add vlan base on the existent vlan Remove: remove-vlan-list, remote vlan base on the existent vlan
4	**switchport hybrid untagged vlan { all** | *vlan-list* | **add** *add-vlan-list* | **remove** *remove-vlan-list***}**	Configure the allowed VLANs for the Untagged port All: allow all vlan vlan-list: allow all VLAN, rewrite the primary configuration Add: add-vlan-list: add vlan base on the existent vlan Remove: remove-vlan-list, remote vlan base on the existent vlan
5	**exit**	Back to global configuration mode
6	**exit**	Back to privileged EXEC mode
7	**show interface port** [{*1-26*}] **switchport**	Show the port VLAN attributes configuration

Use **no switchport hybrid allowed vlan** to restore Hybrid port allowed VLAN to default value, that is, all the VLAN is allowed to pass.

Use **no switchport hybrid untagged vlan** to restore Hybrid port allowed Untagged VLAN to default value, that is, only VLAN is allowed to pass.

4. Configure VLAN that is allowed to pass Trunk port, the steps are as follows:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface port** *portid*	Enter corresponding physical port configuration mode
3	**switchport trunk allowed vlan { all** | *vlan-list* | **add** *add-vlan-list* | **remove** *remove-vlan-list***}**	Configure the allowed VLAN for the Trunk port All: allow all vlan vlan-list: allow all VLAN, rewrite the primary configuration Add:

		add-vlan-list: add vlan base on the existent vlan
		Remove: remove-vlan-list，remote vlan base on the existent vlan
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface port** [*port-list*] **switchport**	Show port VLAN attribute configuration

Use **no switchport trunk allowed vlan** to restore Trunk port allowed VLAN list to default value, that is, all the VLAN.

5.   Configure Native VLAN of Trunk and Hybrid port, the steps are as follows:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface port** *portid*	Enter corresponding physical port configuration mode
3	**switchport native vlan** *<1-4094>*	Configure Native VLAN of Trunk and Hybrid port
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface port** [*port-list*] **switchport**	Show port VLAN attribute configuration

Use **no switchport native vlan** to restore Native VLAN of Trunk and Hybrid port to default value, or VLAN1.

15.2.1.6 VLAN filtration enable/disable function

The configuration of VLAN filtration enable/disable function is shown below:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface port** *portid*	Enter corresponding physical port configuration mode
3	**switchport ingress-filtering** *(enable/ disable)*	Configure port VLAN filtration attribute : enable/diable
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface port** [*port-list*] **switchport**	Show port VLAN attribute configuration

15.2.1.7 Configure port protection

The configuration steps are as follows:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface port** *portid*	Enter corresponding physical port configuration mode
3	**switchport protect**	Configure the physical port to protected port **Protect** the protected port
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface port protected**	Show physical port protection attribute

Use **no switchport protect** to cannel port protection configuration.

15.2.1.8 Configure port transmission

By default, the port can transmit messages to other ports except its own one, port transmission function supports port list configuration under port, so that the range of the ports that are able to transmit messages can be confined.

To configure transmission port, you need to enter the given port or port range mode, the corresponding commands are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	**interface port** *portid*	Enter port mode
3	**switchport forwarding allowed portlist** *port-list*	Configure transmission list under port *Port-list*: port list
4	**exit**	Quit from interface mode
5	**exit**	Quit from global configuration mode
6	**show interface port** [*port-list*] switchport	Show port transmission list

Use **no switchport forwording allowed portlist** to restore port transmission list to default value, that is, all the ports except its own one.

15.2.1.9 Monitoring and maintenance

Command	Command parameter introduction
show interface port [*port-list*] **switchport**	Show port VLAN attribute configuration
show interface port protected	Show physical port protection attribute
show vlan	Show port VLAN attribute configuration

15.2.1.10 Typical configuration example

The topology structure is shown below:
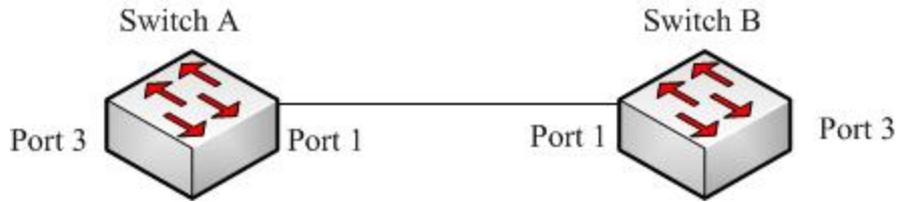
Fig 1 topology structure

As is shown in figure 1, the SwitchA and SwtichB use Port1(SwtichA) and Port1(SwitchB) to connect each other, configure Port1 of the two equipments to Trunk port, allowVLAN1-VLAN100 to pass, Port3(SwtichA) and Port3(SwtichB) are Access port, Access VLAN is VLAN6. The configuration of SwitchA and SwitchB are totally the same, now SwitchA configuration will be shown.

SwitchA configuration is as follows:

Raisecom#**config**

Raisecom(config)#**vlan** *6*

Raisecom(config-vlan)#**state** *active*

Raisecom(config-vlan)#**exit**

Raisecom(config)#**interface port** *1*

Raisecom(config-port)#**switchport mode trunk**

Raisecom(conifg-port)#**switchport trunk allowed vlan** *1-100*

Raisecom(config-port)# **exit**

Raisecom(config)#**interface port** *3*

Raisecom(config-port)#**switchport mode access**

Raisecom(config-port)# **switchport access vlan** *6*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show vlan**

Outer TPID: 0x9100

VLAN	Name	Status	VLAN-Priority	Ports
1	Default	active	N/A	1,2,4-26
6	VLAN0006	active	0	3

Raisecom#**show interface port** *1* **switchport**

Port 1:

Administrative Mode: trunk

Operational Mode: trunk

Access Mode VLAN: 1(default)

Tunnel Mode VLAN: 1(default)

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-100

Operational Trunk Allowed VLANs: 1,3-100

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

Raisecom#**show interface port** *3* **switchport**

Port 3:

Administrative Mode: access

Operational Mode: access

Access Mode VLAN: 6

Tunnel Mode VLAN: 6

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

15.2.2   VLAN mapping function

VLAN mapping offers CVID for message modification, if the equipment has configured the corresponding mapping rules, the new CVID or SVID that has been mapped will do learning and transmission as transmission VLAN.

15.2.2.1 Default VLAN mapping configuration

Function	Default value
Enable/disable port VLAN mapping function	Disable to all

15.2.2.2 Configure VLAN mapping

The steps to enable/disable VLAN mapping function and configure VLAN Mapping rules are shown below:

Step	Command	Command parameter explain
1	**config**	Enter global configuration mode
2	**vlan-mapping** *vlan-list1* **to** *vlan-list2*	Configure VLAN mapping rule *Vlan-list1* the VLAN ID before mapping *Vlan-list2* the VLAN ID afeter mapping
3	**interface port** *portid*	Enter interface configuration mode
4	**vlan-mapping** *{enable|disable}*	Enable VLAN mapping function *Enable* enable VLAN mapping *Disable* disable VLAN mapping
5	**exit**	Quit from physical port mode
6	**exit**	Quit from global configuration mode
7	**show vlan-mapping**	Show VLAN mapping rules
8	**show port** {*all|port-list*} **vlan-mapping**	Show all/specified port VLAN mapping function state *All:* all the ports *Port-list*: the specified port or port list

Notice:

➢ If the number relationship of vlan-list1 and vlan-list2 is N(N>1) to 1, the command will map several VLAN to one VLAN; if it is N to N, then vlan-list1 and vlan-list2 need to be the same in amount in configuration, when doing VLAN mapping the principle of one-one correspondence.
➢ By default VLAN mapping function is disabled. When VLAN mapping function of the specified port is enabled, the corresponding mapping rule will take effect on the port.

15.2.2.3 Monitoring and maintainenance

Command	Command parameter introduction
show interface port [*port-list*] **switchport**	Show the transmission list under specified port
show vlan-mapping	Show VLAN mapping rules
show port {*all|port-list*} **vlan-mapping**	Show all/ the specified ports VLAN mapping function state *All:* all the ports *Port-list*: specified port or port list

15.2.2.4 Typical configuration example

The topology structure is shown in figure 2:
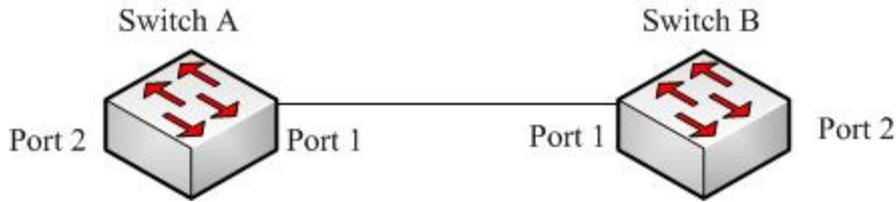
Fig 2 the topology structure

As is shown in figure 2, SwitchA and SwitchB use port 1 for connection, the Port1 and Port2 of the two equipments are both trunk port, create VLAN10-20 and 110-120, map vlan10-20 to vlan110-120, enable VLAN mapping function on Port2. The configuration of SwtichA and SwitchB is totally the same, now SwtichA configuration will be shown.

The configuration of SwitchA:

Raisecom#**config**

Raisecom(config)#**create vlan** *10-20, 110-120 active*

Raisecom(config)# **vlan-mapping** *10-20 to 110-120*

Raisecom(config)#**interface port** *1*

Raisecom(config-port)# **switchport mode trunk**

Raisecom(config-port)#**exit**

Raisecom(config)# **interface port** *2*

Raisecom(config-port)# **switchport mode trunk**

Raisecom(config-port)#**vlan-mapping** *enable*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show vlan-mapping**

Global vlan mapping rules:

Original VLAN IDs   Translated VLAN IDs

10-20   110-120

Raisecom#**show port** *1-2* **vlan-mapping**

Vlan Mapping Status:

PORT   VLAN-MAPPING STATUS

----

1   disable

2   enable

15.2.3 Basic Q-IN-Q function

15.2.3.1 Default Q-IN-IN configuration

Function	Default value
Configure TPID value of outer layer Tag is HHHH	Default TPID value of outer layer Tag is 0x9100
Configure the port ACCESS VLAN ID	1
Configure port VLAN mode	All the ports exists in ACCESS mode in VLAN1.

15.2.3.2 Basic Q-IN-Q configuration

The steps of configuring Q-IN-Q includes: Tpid, access vlan, tunnel port and double tagging configuration, as is shown below:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**mls double-tagging tpid** *HHHH*	Configure the outer layer Tag TPID value to HHHH; *HHHH:* hex outer layer Tag TPID value, it is 1~4 figures hex number, range is 0x0-0xFFFF.
3	**interface port** *portid*	Enter port mode
4	**switchport mode** *{access | hybrid [double-tagging|dot1q-tunnel]|trunk [double-tagging]| dot1q-tunnel [hybrid]}*	Configure port VLAN mode **access** ACCESS mode, port exists in the form of UNTAG in the only VLAN; **hybrid** HYBRID mode, the port can exist in several VLAN in UNTAG or TAG mode; **hybrid double-tagging** configure the port to HYBRID mode, so that it can recognize and handle outer layer Tag (SP VLAN Tag); **hybrid dot1q-tunnel** configure the port to HYBRID mode, can make it enable to compulsively adding outer layer Tag(SP VLAN Tag) for the packet entering the port; **trunk** TRUNK mode, the port exists in several VLAN in TAG mode, and exists in Native Vlan in UNTAG mode; **trunk double-tagging** configure the port to TRUNK mode, and enable it the ability to recognize and handle outer layer Tag; **dot1q-tunnel** TUNNEL mode, the data packet entering the port can be added double Tag.
4	**switchport access vlan** *<1-4094>*	Configure the port ACCESS VLAN ID. *<1-4094>* specific port's ACCESS VLAN ID in ACCESS and DOT1Q-TUNNEL mode.
5	**exit**	Return to global configuration mode
6	**show vlan**	Show VLAN configuration
7	**show interface port** [*port-list*] **switchport**	Show port VLAN attribute information

Use **no mls double-tagging tpid HHHH** to restore outer layer Tag TPID to default value:0x9100.

Use **no switchport mode** to restore port VLAN mode to default value, that is ACCESS mode.

Use **no switchport access vlan** mode to restore Access VLAN to default value, that is, port Access VLAN is VLAN 1.

15.2.3.3 Monitoring and maintenance

Command	Command parameter instruction
show vlan [{*1-4094*}]	Show stable VLAN configuration
show interface port [*port-list*] **switchport**	Show port VLAN attribute configuration

15.2.3.4 Typical configuration example

The topology structure is shown in figure 3:
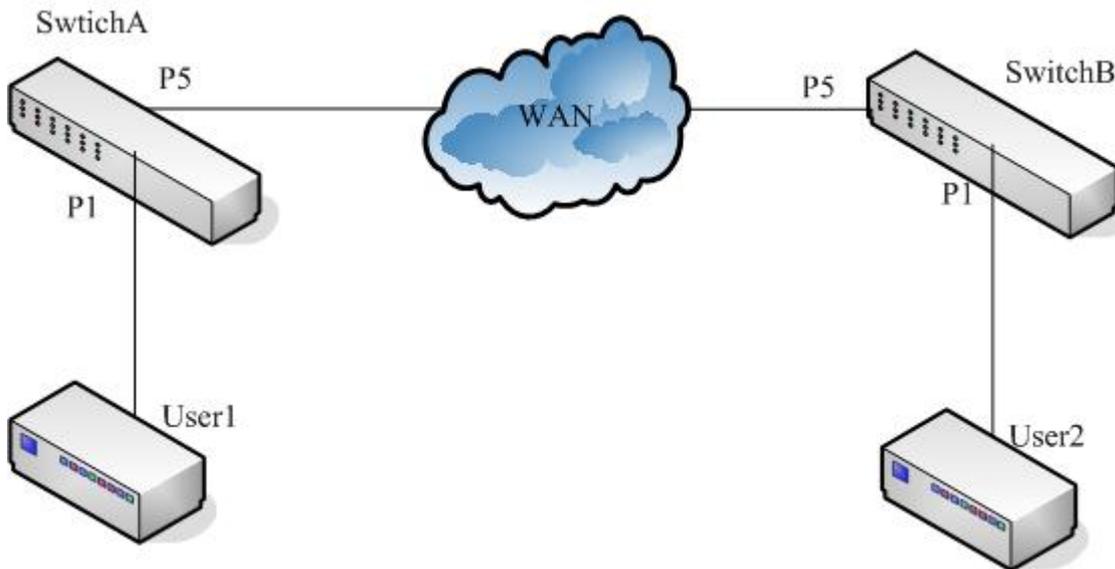
Fig 3 topology structure

As is shown in figure 3, SwitchA and SwitchB are operator's access switches, belong to operator network's VLAN100 and VLAN200 respectively. User1 and User2 are user access equipment, SwitchA use P5 port to connect to MAN (metro area network), p1 port connect ot User1, SwitcB use P5 to connect to MAN. P1 connect to User2. MAN TPID is ox8600. Configure SwitchA and SwtichB to realize QinQ function.

SwitchA configuration is shown below:

Raisecom#**config**

Raisecom(config)#**mls double-tagging** *tpid 8600*

Raisecom(config)#**interface port** *1*

Raisecom(config-port)#**switchport mode** *dot1q-tunnel*

Raisecom(config-port)#**switchport access vlan** *100*

Raisecom(config-port)#**exit**

Raisecom(config)#**interface port** *5*

Raisecom(config-port)#**switchport mode** *trunk double-tagging*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show interface port** *1* **switchport**

Port 1:

Administrative Mode: dot1q-tunnel

Operational Mode: dot1q-tunnel

Access Mode VLAN: 100

Tunnel Mode VLAN: 100

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

Raisecom#**show interface port** *5* **switchport**

Port 5:

Administrative Mode: trunk double-tagging

Operational Mode: trunk double-tagging

Access Mode VLAN: 1(default)

Tunnel Mode VLAN: 1(default)

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: 1,100

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

SwitchB configuration is shown below:

Raisecom#**config**

Raisecom(config)#**mls double-tagging** *tpid 8600*

Raisecom(config)#**interface port** *1*

Raisecom(config-port)#**switchport mode** *dot1q-tunnel*

Raisecom(config-port)#**switchport access vlan** *200*

Raisecom(config-port)#**exit**

Raisecom(config)#**interface port** *5*

Raisecom(config-port)#**switchport mode** *trunk double-tagging*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show interface port** *1* **switchport**

   Port 1:

   Administrative Mode: dot1q-tunnel

   Operational Mode: dot1q-tunnel

   Access Mode VLAN: 200

   Tunnel Mode VLAN: 200

   Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

   Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

   Administrative Trunk Allowed VLANs: 1-4094

   Operational Trunk Allowed VLANs: n/a

   Administrative Hybrid Allowed VLANs: 1-4094

   Operational Hybrid Allowed VLANs: n/a

   Administrative Hybrid Untagged VLANs: 1

   Operational Hybrid Untagged VLANs: n/a

   Native Mode VLAN: 1(default)

   VLAN Ingress Filtering: Enabled

   switchport forwarding allowed portlist: n/a

Raisecom# **show interface port** *5* **switchport**

   Port 5:

   Administrative Mode: trunk double-tagging

   Operational Mode: trunk double-tagging

   Access Mode VLAN: 1(default)

   Tunnel Mode VLAN: 1(default)

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: 1,200

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

15.2.4 Flexible Q-IN-Q function

15.2.4.1 Default flexible Q-IN-Q configuration

Function	Default value
Configure port flexible Q-IN-Q VLAN mapping relationship	None

15.2.4.2 Configure flexible Q-IN-Q

Flexible Q-in-Q function is to add outer layer TAG according to inner TAG. Configuring port flexible Q-in-Q function must be within physical port configuration mode, the steps are as follows:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface port** *portid*	Enter corresponding physical port configuration mode
3	**switchport vlan mapping** *vlan-list* **add-outer** *outer-vlan-list*	Configure the VLAN mapping relationship of port flexible Q-in-Q *vlan-list* inner: layer VLAN ID from client network *outer-vlan-list*: added outer layer VLAN ID
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show vlan mapping**	Show all the VLAN mapping configuration
7	**show interface port** [*port-list*] **switchport**	Show port VLAN attribute configuration

Use **no switchport vlan mapping** {all | vlan-list} to delete the VLAN mapping relationship of port Q-in-Q.

Notice:

➢ To ISCOM2924GF/2926, 768 VLAN mapping can be configured at the most.
➢ The VLAN mapping relationship of flexible Q-in-Q function configure by this command takes effect only on TUNNEL port, that is, only when the interface mode is TUNNEL, can flexible

Q-in-Q function takes effect. The port enters command configured outer layer VLAN in the way of UGTAG, if VLAN do not exist, it will be created automatically. When deleting one Q-in-Q VLAN mapping relationship, if other mapping do not user this outer layer VLAN, delete the port from outer layer VLAN.

15.2.4.3 Monitoring and maintenance

Command	Command parameter instruction
show vlan mapping	Show all the VLAN mapping configuration
show interface port [*port-list*] **switchport**	Show port VLAN attribute configuration

15.2.4.4 Typical configuration example

The topology structure is shown below:
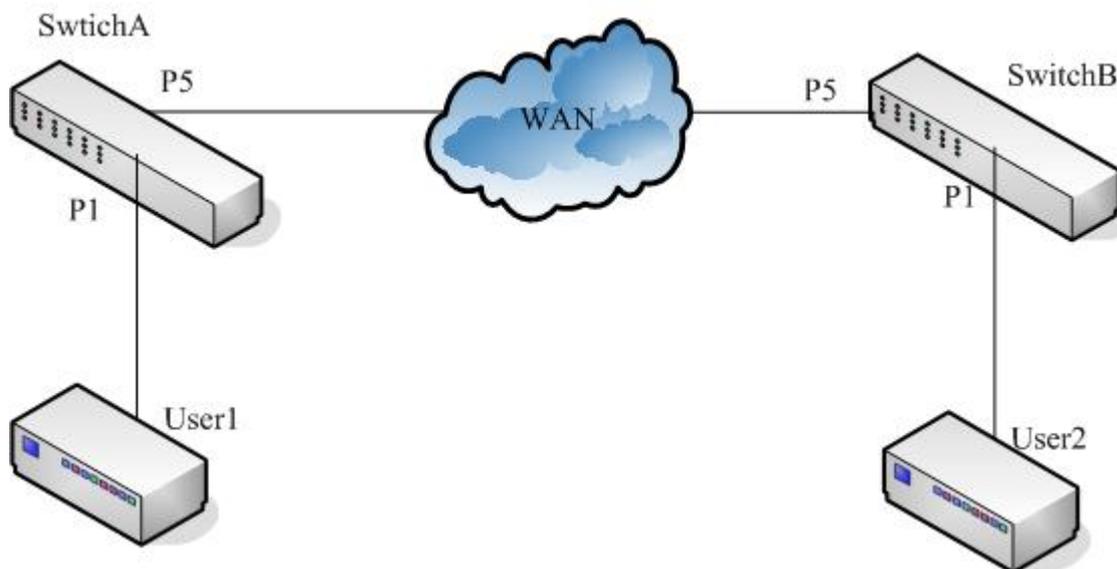
Fig 4 topology structure

As is shown in figure 4, SwitchA and SwitchB are operator access switches, they belong to VLAN 100 and VLAN 200 of the operator's network respectively. User1 and User2 are user access equipments, SwitchA user P5 port to connect to MAN (metro area network), P1 connect to User1, SwtichB connect to MAN using P5, P1 connect to User2. MAN TPID is 0x8600. User1 belongs VLAN10, User2 belong to VLAN20, configure SwitchA and SwitchB to relalize flexible Q-in-Q function.

SwitchA configure is shown below:

Raisecom#**config**

Raisecom(config)#**mls double-tagging** *tpid 8600*

Raisecom(config)#**interface port** *1*

Raisecom(config-port)#**switchport mode** *dot1q-tunnel*

Raisecom(config-port)#**switchport vlan mapping** *10* **add-outer** *100*

Raisecom(config-port)#**exit**

Raisecom(config)#**interface port** *5*

Raisecom(config-port)# **switchport mode trunk double-tagging**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show vlan mapping**

Port	Inner VLAN	Outer VLAN	Hardware
1	10	100	Yes

Raisecom#**show interface port** *1* **switchport**

Port 1:

Administrative Mode: dot1q-tunnel

Operational Mode: dot1q-tunnel

Access Mode VLAN: 4

Tunnel Mode VLAN: 4

Administrative Tunnel Mode OUTER VLANs of vlan mapping: 100

Operational Tunnel Mode OUTER VLANs of vlan mapping: 100

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

Raisecom# **show interface port** *5* **switchport**

Port 5:

Administrative Mode: trunk double-tagging

Operational Mode: trunk double-tagging

Access Mode VLAN: 1(default)

Tunnel Mode VLAN: 1(default)

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: 1,3-6,100

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

SwtichB configuration is shown below:

Raisecom#**config**

Raisecom(config)#**mls double-tagging tpid** *8600*

Raisecom(config)#**interface port** *1*

Raisecom(config-port)#**switchport mode dot1q-tunnel**

Raisecom(config-port)#**switchport vlan mapping** *20* **add-outer** *200*

Raisecom(config-port)#**exit**

Raisecom(config)#**interface port** *5*

Raisecom(config-port)# **switchport mode trunk double-tagging**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show vlan mapping**

Port	*Inner VLAN*	*Outer VLAN*	*Hardware*
1	*20*	*200*	*Yes*

Raisecom#**show interface port** *1* **switchport**

Port 1:

Administrative Mode: dot1q-tunnel

Operational Mode: dot1q-tunnel

Access Mode VLAN: 4

Tunnel Mode VLAN: 4

Administrative Tunnel Mode OUTER VLANs of vlan mapping: 200

Operational Tunnel Mode OUTER VLANs of vlan mapping: 200

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

Raisecom# **show interface port** *5* **switchport**

Port 5:

Administrative Mode: trunk double-tagging

Operational Mode: trunk double-tagging

Access Mode VLAN: 1(default)

Tunnel Mode VLAN: 1(default)

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: 1,3-6,200

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

15.3 VLAN Function Configuration

15.3.1 Configure VLAN

15.3.1.1 Switching mode introduction

Switching mode can be sorted to 3 types:

- **transparent :**transparent mode

- **vlan:** VLAN transmission mode

- **double-tagged-vlan:** Q-in-Q VLAN mode

In transparent mode, stable VLAN and port VLAN configuration do not take effect actually. When the system transforms from transparent mode to VLAN transmission mode, stable VLAN and port VLAN configuration can actually take effect.

In VLAN transmission mode, stable VLAN and port VLAN configuration take effect directly.

15.3.1.2 Default VLAN configuration

Function	Default value
Create VLAN	Default VLAN
Configure switching mode	Transparent mode
Configure the filtration mode of physical port ingress data packet	No ingress be abandoned.
Configure the data packets that are allowed to be received by physical port	All the data packets are allowed to be received
Configure the handling mode of physical port ingress data packet	No modification to outgress data packet

15.3.1.3 Configure switching mode

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**switch-mode** *{transparent/ dot1q-vlan/double-tagged-vlan}*	Configure switching mode **transparent**: transparent mode **vlan**: VLAN transmission mode **double-tagged-vlan:** Q-in-Q VLAN mode
3	**exit**	Return to privileged EXEC mode
4	**show vlan**	Show stable VLAN configuration

Notice:

➢ In transparent mode, stable VLAN and port VLAN configuration do not take effect actually. In this mode, the system record the configuration done by the commands below, but do not actually carry out them:
- Vlan
- Pvid
- Vlan accept-frame
- Vlan double-tag
- Vlan egress default
- Vlan ingress-filtering

➢ When the system transforms from transparent mode to VLAN transmission mode, the configuration commands above can really take effect. In VLAN transmission mode, the configurations above will be carried out and take effect directly.

15.3.1.4 Configure VLAN attribute

VLAN attribute configuration includes creating and deleting VLAN.

1. Create VLAN

Create VLAN, and define if out port is UNTAG port in VLAN member group, the steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration

		Create VLAN
2	**vlan**<2-4094>{**client**[*clientid*]|**line** [*lineid*]} **untagged** {**client** [*clientid*]|**line** [*lineid*]}	Untagged: only out port is allowed to let go data packet without TAG; Client: user end port; Line: line side port *<2-4094>*: VLAN ID; *Clientid:* user port number *lineid* line port number
3	**exit**	Return to privileged EXEC mode
4	**show vlan**	Show VLAN configuration

2. Delete VLAN

When user needs to delete a VLAN, follow the steps below:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**no vlan** {*all* | *<2-4094>*}	Delete VLAN *<2-4094>*: VLAN ID; All: all the stable VLAN except default VLAN (VLAN ID is 1)
3	**exit**	Return to global configuration mode
4	**show vlan**	Show VLAN configuration

15.3.1.5 Enable/disable VLAN filtration

The steps to configure the physical port ingress data packet filtration mode are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {client** *clientid* | **line** *lineid*}	Enter corresponding physical port configuration mode
3	**vlan ingress-filtering** {**unknown-vlan**| **not-member**}	Configure the filtration mode of physical port ingress data packet
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface {client** *client-list* | **line** *line-list*} **switchport**	Show VLAN configuration

Use **no vlan ingress-filtering** to restore ingress data packet filtration mode to default value, that is, no ingress packet will be dropped.

15.3.1.6 Configure VLAN accept-frame tagging type

The steps to configure VLAN accept-frame tagging type are as follows:

Step	Command	Command parameter instruction
1	**config**	Enter global configuration mode
2	**interface {client** *clientid* **| line** *lineid*}	Enter corresponding physical port configuration mode
3	**vlan accept-frame** *{tag|untag}*	Configure physical port accepted data packet Tag: accept only the data packets with TAG Untag: accept only the data packet without TAG
4	exit	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface {client** *client-list* **| line** *line-list*} **switchport**	Show VLAN configuration

Use **no vlan accept-frame** to restore VLAN accept-frame tagging type to default value, that is, all the data packets are allowed to receive.

15.3.1.7 Configure outgress mode

The steps to configure the processing mode of physical port outgress data packet are as follows:

Step	Command	Command parameter instruction
1	**config**	Enter global configuration mode
2	**interface {client** *clientid* **| line** *lineid*}	Enter corresponding physical interface configuration mode
3	**vlan egress default** *{tag| untag | unmodify}*	Configure the processing mode to physical port outgress data packets **Tag** outgress data packet adding TAG **Untag** outgress data packet without TAG **Unmodify** do not modify outgress data packet
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface {client** *client-list* **| line** *line-list*} **switchport**	Show VLAN configuration

Notice:

➢ If double TAG function is enabled on physical port, the processing mode to physical port outgress data packet will not take effect.

15.3.1.8 Configure PVID

The steps to create and delete port VLAN ID are shown below:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration

2	**interface {client** *clientid* **| line** *lineid***}**	Enter corresponding physical configuration mode
3	**[no] pvid** *<1-4094> [override]*	Create and delete port VLAN ID *<1-4094>*: port VLAN ID number *override*: use PVID value to recover the VLAN ID in the message
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface {client** *client-list* **| line** *line-list***} switchport**	Show VLAN configuration

Use **no pvid** to delete PVID.

15.3.1.9 Monitoring and maintenance

Command	Description
show vlan [{*1-4094*}]	Show stable VLAN configuration
show interface client [*client-list*] **switchport**	Show user port VLAN configuration
show interface line [*line-list*] **switchport**	Show line port VLAN configuration

15.3.1.10 Typical configuration example

Topology structure is shown as figure 5:
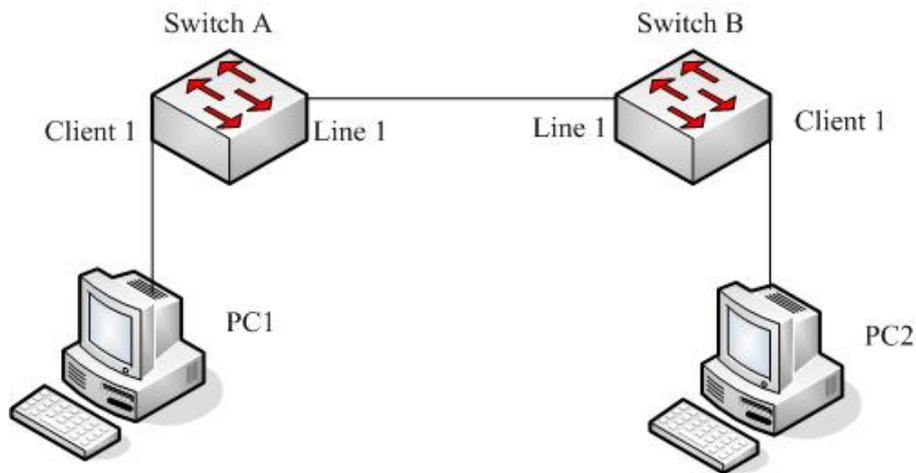
Fig 5 topology structure

As is shown in figure 5, Line1 of SwtichB connects with Line1 of SwtichA, configure SwitchA switching mode to vlan transmission mode, and configure Client1 outgress data packet filtration and VLAN accept-frame tagging type.

SwitchA configuration is shown below:

Raisecom#**config**

Raisecom(config)#**vlan** *3* **line** *1* **client** *1*

Raisecom(config)#**switch-mode dot1q-vlan**

Raisecom(config)#**interface client** *1*

Raisecom(config-port)#**vlan accept-frame** *untag*

Raisecom(config-port)#**vlan egress default** *untag*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show vlan**

Switch mode: dot1q-vlan

Core tag type: 0x9100

VLAN   Ports   Untag Ports   Priority

 ---

1   L:1;C:1   L:1;C:1   --

3   L:1;C:1   n/a   --

Raisecom#**show interface client** *1* **switchport**

Port client1:

PVID: 1

PVID override: Disabled

Double tag: Disabled

Vlan accept-frame: Untagged

Vlan ingress filtering: None

Egress default : Untagged

SwitchB configuration is shown below:

Raisecom#**config**

Raisecom(config)#**vlan** *3-5* **line** *1* **client** *1*

Raisecom(config)#**switch-mode dot1q-vlan**

Raisecom(config)#**interface client** *1*

Raisecom(config-port)#**vlan accept-frame** *untag*

Raisecom(config-port)#**vlan egress default** *untag*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show vlan**

Switch mode: dot1q-vlan

Core tag type: 0x9100

VLAN   Ports   Untag Ports   Priority

 ---

1   L:1;C:1   L:1;C:1   --

3   L:1;C:1   n/a   --

4   L:1;C:1   n/a   --

Raisecom#**show interface client** *1* **switchport**

Port client1:

PVID: 1

PVID override: Disabled

Double tag: Disabled

Vlan accept-frame: Untagged

Vlan ingress filtering: None

Egress default : Untagged

15.3.2 Basic Q-in-Q function

15.3.2.1 Basic Q-in-Q default configuration

Function	Default value
Configure outer layer Tag TPID value	The default TPID value of outer layer Tag is 0x9100
Enable/disable physical port double TAG function	Double TAG function is disabled

15.3.2.2 Configure basic Q-in-Q

Q-in-Q configuration includes: switching mode, Tpid, PVID and double tagging configuration, the configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**switch-mode** *{ transparent/ dot1q-vlan/double-tagged-vlan}*	Configure switching mode to double-tagged-vlan mode **Transparent:** transparent mode **Vlan**: VLAN Transmission mode **double-tagged-vlan**: Q-in-Q VLAN mode
3	**mls double-tagging tpid** *HHHH*	Configure outer layer Tag TPID value to HHHH *HHHH:* hex outer layer Tag TPID value, which is 1~4 figures hex number, range is 0x0-0xFFFF
4	**interface {client** *clientid* **| line** *lineid***}**	Enter corresponding physical interface configuration mode
5	**pvid** *<1-4094> [override]*	Create port VLAN ID *<1-4094> :* port VLAN id override*:* use PVID value to recover message VLAN ID
6	**vlan double-tag**	Enable physical port double TAG function
7	**exit**	Return to global configuration mode
8	**exit**	Return to privileged EXEC mode

9	**show vlan**	Show stable VLAN configuration
10	**show interface {client** *client-list* **| line** *line-list***} switchport**	Show VLAN configuration

Use **no mls double-tagging tpid HHHH** to restore outer layer Tag TPID to default value, 0x9100.

Use **no vlan double-tag** to stop physical port double TAG function.

15.3.2.3 Monitoring and maintenance

Command	Description
show vlan [{*1-4094*}]	Show stable VLAN configuration
show interface client [*client-list*] **switchport**	Show user port VLAN configuration
show interface line [*line-list*] **switchport**	Show line port VLAN configuration

15.3.2.4 Typical configuration example

Topology structure:
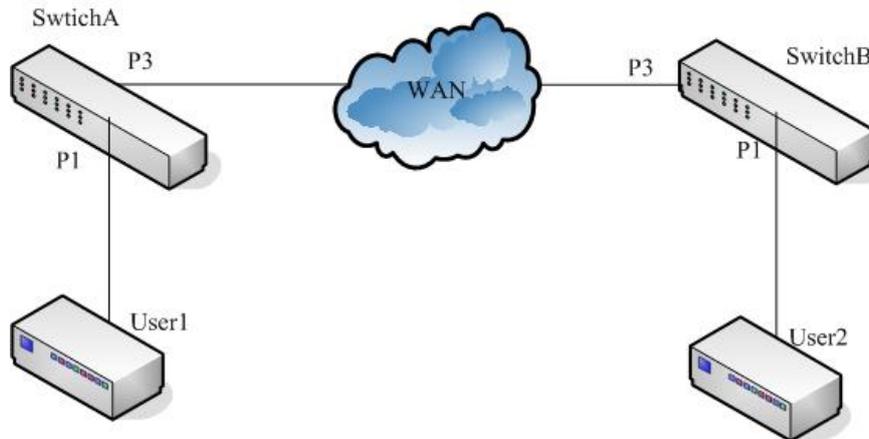
Fig 6 topology structure

As is shown in the topology structure, SwitchA and SwtichB are operator access switches, which belongs to VLAN100 and VLAN200 of the operator network. User1 and User2 are user access equipments, SwitchA use P5 to connect to MAN (metro area network), P1 connect to User1, SwitchB use P5 to connect to MAN, P1 connect to User2. Among them, MAN TPID is 0x9600. Configure SwtichA and SwtichB to realize basic Q-in-Q function.

SwitchA configuration is as follows:

Raisecom#**config**

Raisecom(config)#**switch-mode double-tagged-vlan**

Raisecom(config)#**mls double-tagging tpid** *9600*

Raisecom(config)#**interface client** *3*

Raisecom(config-port)#**pvid** *100*

Raisecom(config-port)#**vlan double-tag**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show vlan**

Switch mode: double-tagged-vlan

Core tag type: 0x9600

VLAN	Ports	Untag Ports	Priority
1	L:1;C:1-4	L:1;C:1-4	--
3	C:3	n/a	--
5	L:1	n/a	--

Raisecom#**show interface client** *3* **switchport**

Port client3:

PVID: 100

PVID override: Disabled

Double tag: Enabled

Vlan accept-frame: All

Vlan ingress filtering: None

Egress default : Unmodify

SwitchB configuration is as follows:

Raisecom#**config**

Raisecom(config)#**switch-mode double-tagged-vlan**

Raisecom(config)#**mls double-tagging tpid** *9600*

Raisecom(config)#**interface client** *3*

Raisecom(config-port)#**pvid** *200*

Raisecom(config-port)#**vlan double-tag**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show vlan**

Switch mode: double-tagged-vlan

Core tag type: 0x9600

VLAN	Ports	Untag Ports	Priority
1	L:1;C:1-4	L:1;C:1-4	--
5	L:1	n/a	--
6	C:2	n/a	--

Raisecom#**show interface client** *3* **switchport**

Port client3:

PVID: 200

PVID override: Disabled

Double tag: Enabled

Vlan accept-frame: All

Vlan ingress filtering: None

Egress default : Unmodify

15.4 VLAN configuration

15.4.1　VLAN based on port

The device switch mode can be configured into two types, transparent mode and dot1q-vlan mode.

In transparent mode, static VLAN and VLAN configuration under port does not actually work. Only when the system transforms from transparent mode to dot1q-vlan mode can static VLAN and port VLAN configuration under port takes effect.

In dot1q-vlan mode, static VLAN and VLAN configuration under port takes effect directly.

15.4.1.1 VLAN port mode introduction

Member port mode	VLAN member attribution
ACCESS	In Access mode, by default only VLAN1 data packets are allowed to pass the port, and the data packets sent from the port do not take VLAN 1 tag. Access port mode can be designated to multi-VLAN, but the data packets sent from access port do not take VLAN tag. Access port is mainly used to connect terminal user.
TRUNK	In trunk mode, all the VLAN packets are allowed to pass by default, and all the data packets except VLAN 1 transmitted from the have tag. Trunk mode can be designated to multi-VLAN, and user can configure if the data packet with a certain VLAN tag should be transmitted from the port. When the switch is used as the uplink tag port, it can be configured to trunk mode

15.4.1.2 Default VLAN configuration

Function	Default value
Device switch mode	transparent
Create static VLAN	Default VLAN and cluster VLAN exist in the system, that is VLAN1 and VLAN2, all the ports exist in VLAN1.
VLAN name	System default VLAN name is 'default', other static VLAN name is 'VLAN' added its 4 figures VLAN ID
Static VLAN activity state	Newly created static VLAN activity state is suspend.
VLAN priority	No priority

Port mode	Access
ACCESS VLAN	VLAN 1
ACCESS VLAN override	Disable
The VLAN that is allowed to pass the port in access mode	VLAN 1
The Native VLAN of trunk port	VLAN 1
The VLAN that is allowed to pass VLAN in port VLAN mode	All VLAN
The UNTAG VLAN that is allowed to pass VLAN in port trunk mode	VLAN 1

15.4.1.3 Configure switch mode

Step	Command	Description
1	**config**	Enter global configuration mode
2	**switch-mode** *{transparent| dot1q-vlan}*	Configure switch mode
3	**exit**	Return to privileged EXEC mode
4	**show vlan**	Show static VLAN configuration

Attention:

➢ In transparent mode, the device transmits data packets without the limitation of VLAN, the system records but do not actually execute the following configuration:
   ● Static VLAN will be created and enabled
   ● VLAN priority
   ● Port access VLAN and override
   ● Port access egress-allowed VLAN
   ● Port trunk native VLAN
   ● Port trunk allow VLAN, port trunk untag VLAN
   ● Port mode
   ● QinQ configuration

15.4.1.4 Configure VLAN attribution

VLAN attribution includes to create, delete VLAN, configure VLAN name, priority, and active state. The steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**create vlan** {2-4094} **(active|suspend) [priority** <0-7>]	Create VLAN, confirm the state (active/suspend),configure the priority Active: active state

		Suspend: hang-up state
		0-7: VLAN priority
		{2-4094}: VLAN ID
3	**name** *WORD*	Name VLAN
		WORD VLAN name, no longer than 15 characters
4	**state** *{active | suspend}*	Configure VLAN activity state
5	**exit**	Return to global configuration mode
6	**exit**	Return to privileged EXEC mode
7	**show vlan**	Show VLAN configuration

Use **no vlan** *<2-4094>* to delete VLAN in global configuration mode.

Attention:

➢ The newly created VLAN using VLAN <1-4094> is in suspend state, if user hopes to make it active in the system, the command **state** that will be introduced later can help.
➢ By default there are two VLAN in the system, that is default VLAN (VLAN1) and cluster VLAN (VLAN2), all the ports belongs to the default VLAN. Default VLAN is not allowed to be deleted. To learn more about cluster VLAN, ref. 19-cluster management function.
➢ By default, the default VLAN (VLAN1) name is 'Default', other static VLAN name is 'VLAN' added with 4 figure VLAN ID, for example the default name of VLAN 3is 'VLAN0003', the default name of VLAN 4094 is 'VLAN4094'.
➢ Only when a VLAN be activated in the system can it be active. When VLAN active status is suspend, user can configure the VLAN, like to delete/add port, configure VLAN priority, the system will keep the configuration, once the VLAN is activated, the configuration will take effect in the system.

15.4.1.5 Configure VLAN priority

By default, there is no priority when creating VLAN, N/A will be shown, VLAN priority range is 0-7. The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**vlan** *<1-4094>*	Create VLAN and enter its configuration mode
		<1-4094> VLAN ID
3	**priority** *<0-7>*	Configure VLAN priority
		0-7: VLAN priority
4	**exit**	Return to privileged EXEC mode
5	**show vlan**	Show VLAN configuration

Use **no vlan***{2-4094}* **priority** in global configuration mode, or **no priority** in VLAN mode to delete VLAN priority.

Attention:

➢ Default VLAN (VLAN1) has no configuration priority.

- The new created VLAN has no priority be default, and shows N/A. VLAN priority range is 0-7.
- VLAN priority takes effect only when the VLAN is activated. When VLAN is not created or when the state is suspend, user can configure the VLAN priority for still, and the system will keep the configuration and enable the configuration when the VLAN is activated.
- When VLAN priority is configured, the device uses VLAN priority to form a queue or cover message COS value when transmitting VLAN messages. Use **mls qos vlan (priority-set | cos-voerride)** and **mls qos vlan priority-set cos-override** for specific configuration. If VLAN priority is deleted or if VLAN is not activated, the commands above will not take effect either. Ref. 27-QoS configuration guide for QoS commands.

15.4.1.6 Configure port VLAN mode

Port VLAN mode configuration includes port mode, ACCESS VLAN, ACCESS mode allowed VLAN list, TRUNK local VLAN, TRUNK allowed VLAN list, TRUNK UNTAG VLAN list and so on.

You must to configure port VLAN mode in physical interface configuration mode, the steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** *portid*	Enter corresponding physical interface configuration mode
3	**switchport mode {access	trunk}**	Configure port VLAN mode
4	**switchport access vlan** *<1-4094>* **[override]**	Configure port ACCESS VLAN 1-4094: VLAN ID Override: VLAN override
5	**Switchport access egress-allowed vlan** { **all**	*vlan-list*	**add** *add-vlan-list*	**remove** *remove-vlan-list*}	Configure the VLAN that Access port allows to pass **All**, all the VLAN are allowed to pass; *Vlan-list*, VLAN that is allowed to pass, the existed configuration will be covered directly **Add** *add-vlan-list*, add allowed VLAN on the base of existed allowed VLAN **Remove** *remove-vlan-list*, delete allowed VLAN on the base of existed allowed VLAN
6	**switchport native vlan** *<1-4094>*	Configure Native VLAN for Trunk port
7	**switchport trunk allowed vlan** { **all**	*vlan-list*	**add** *add-vlan-list*	**remove** *remove-vlan-list*}	Configure the VLAN that is allowed to pass Trunk port **All** allow all the VLAN to pass *Vlan-list*, allow the passed VLAN ,cover the existed configuration directly; **Add** *add-vlan-list*, add allowed VLAN on the base of the existed allowed VLAN **Remote** *remote-vlan-list*, delete allowed VLAN on the base of the existed allowed VLAN
8	**switchport trunk untagged vlan** { **all**	*vlan-list*	**add** *add-vlan-list*		Configure the Untagged VLAN that is allowed to pass Trunk port,

	remove *remove-vlan-list***}**	**All**, all the VLAN are allowed to pass;
		Vlan-list, the VLAN that are allowed to pass, the existed configuration will be covered directly
9	**exit**	Return to global configuration mode
10	**exit**	Return to privileged EXEC mode
11	**show interface port** *[port-list]* **switchport**	Show port VLAN attribution configuration

Use **no switchport mode** to restore port VLAN to default value. Use **no switchport access vlan** to restore Access VLAN to default value, which is to configure port Access VLAN to VLAN1. Use **no switchport trunk native vlan** to restore the Native VLAN of Trunk port to default value, or VLAN1. Use **no switchport trunk allowed vlan** to restore the VLAN that is allowed to pass through Trunk port to default value, all the VLAN can pass. Use **no switchport trunk untagged vlan** to restore the Untagged VLAN that is allowed to pass Trunk port, only VLAN1 shall pass.

When the user is configured the VLAN or UNTAG VLAN that is allowed to pass, user will be noticed 'please input 'y' to confirm the allowed VLAN', input 'y/Y' or press ENTER directly for confirmation, then the configured value will take effect, or the configuration will not take effect when user input other value.

Notice:

➢ By default, all the ports allow default VLAN (VLAN1) to pass, and all the data packets of the default VLAN transmitted from the ports do not take the corresponding VLAN TAG.
➢ In port Access mode, no matter how the VLAN list that is allowed to pass Access port is configured, the port allows the data packets of Access VLAN to pass, and the packets sent out do not take corresponding VLAN TAG.
➢ In port Access mode, when configuring Access VLAN, if the VLAN is not created and activated, the system will create and enable the VLAN automatically.
➢ In port Access mode, if Access VLAN is deleted or hanged up by user, the system will configure the port Access VLAN to default VLAN (VLAN1).
➢ In port Trunk mode, no matter the configuration of the VLAN list that is able to pass Trunk port and Untagged VLAN list, the port allows the data packets of NATIVE VLAN to pass, and the transmitted data packets do not take corresponding VLAN TAG.
➢ In port Trunk mode, when configured Native VLAN, if the VLAN is not created or enabled, the system will create and enable the VLAN automatically.
➢ In port Trunk mode, if Native VLAN is deleted or blocked by user, the system will set the port Trunk Native VLAN to default VLAN (VLAN1) automatically.
➢ In port Trunk mode, if the configured Native VLAN is not default VLAN, while the VLAN list that allows passing Trunk port includes not default VLAN, then the port will not allow default VLAN data packets pass.
➢ Configuring Trunk allowed VLAN list and Trunk Untagged VLAN list is related. When configuring Trunk allowed VLAN list, the system will delete the not allowed VLAN in Trunk Untagged VLAN list; when configuring Trunk Untagged VLAN list, the system will add all Untagged VLAN to Trunk allowed VLAN.
➢ Access VLAN and Trunk Native VLAN can not be configured to cluster VLAN.
➢ The VLAN list that is allowed to pass Access port, Trunk allowed VLAN list and Trunk Untagged VLAN list takes effect only to static VLAN, not to cluster VLAN, GVRP static VLAN.

15.4.1.7 Configure port protection

The steps are as follows:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**interface port** *portid*	Enter corresponding physical interface configuration mode
3	**switchport protect**	Configure physical port to protected port **Protect** protected port
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface port protected**	Show physical port protection attribution

Use **no switchport protection** to cancel port protection configuration.

15.4.1.8 Configure port forwarding

By default, the port is able to transmit messages to all other ports except to the port itself. The function supports configuring port list under port to limit the port range that could transmit messages.

To configure forwarding port, you need to enter the designated port or range port mode, the commands are shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** *portid*	Enter port mode
3	**switchport forwarding allowed portlist** *port-list*	Configure port forwarding list
4	**exit**	Quit from port mode
5	**exit**	Quit from global mode
6	**show interface port [*port-list*] switchport**	Show port forwarding list

Use **no switchport forwarding allowed** *portlist* to restore the forwarding list under port to default value, that is all the other ports except the port itself.

15.4.1.9 Monitoring and maintenance

Command	Description
show interface port [*port-list*] switchport	Show port VLAN attribution configuration
show interface clinet clinetid switchport	Show the client port VLAN attribution
show interface line lineid switchport	Show line port VLAN attribution
show interface port protected	Show the protected port attribution of the physical port

15.4.1.10 Typical configuration

The topology:
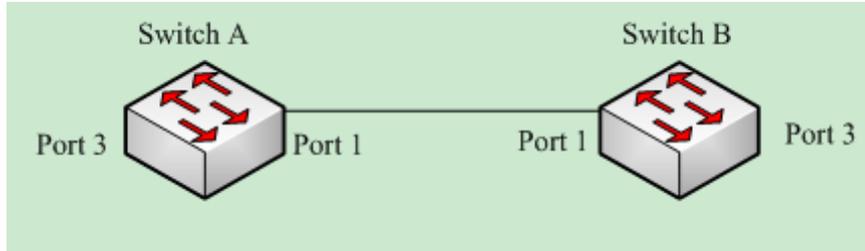
As is shown in the figure above, SwitchA and SwtichB use Port1(SwitchA) and Port1(SwitchB) to connect each, configure Port1 of the two devices to Trunk port, allowing VLAN1-VLAN100, configure Port3(SwitchA) and Port3(SwitchB) to Access port, Access VLAN to VLAN6. The configuration of SwitchA and SwtichB is totally the same. The configuration step of SwtichA is shown below:

Configuration of SwitchA:

Raisecom#**config**

Raisecom(config)#**vlan 6**

Raisecom(config-vlan)#**state active**

Raisecom(config-vlan)#**exit**

Raisecom(config)#**interface port 1**

Raisecom(config-port)#**switchport mode trunk**

Raisecom(conifg-port)#**switchport trunk allowed vlan 1-100**

Raisecom(config-port)# **exit**

Raisecom(config)#**interface port 3**

Raisecom(config-port)#**switchport mode access**

Raisecom(config-port)# **switchport access vlan 6**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show vlan**

VLAN	Name	State	Status	Ports	Untag Ports	Priority	Creation Time
1	Default	active	static	1-26	1-26	--	0:0:32
2		active	other	1-26	n/a	--	0:0:35
6	VLAN0006	active	static	1,3	3	--	4:32:23

Raisecom#**show interface port 1 switchport**

Port 1:

Administrative Mode: trunk

Operational Mode: trunk

Access Mode VLAN: 1

Administrative Access Egress VLANs: 1

Operational Access Egress VLANs: n/a

Trunk Native Mode VLAN: 1

Administrative Trunk Allowed VLANs: 1-100

Operational Trunk Allowed VLANs: 1,6

Administrative Trunk Untagged VLANs: 1

Operational Trunk Untagged VLANs: 1

Raisecom#**show interface port 3 switchport**

Port 3:

Administrative Mode: access

Operational Mode: access

Access Mode VLAN: 6

Administrative Access Egress VLANs: 1

Operational Access Egress VLANs: 1,6

Trunk Native Mode VLAN: 1

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Trunk Untagged VLANs: 1

Operational Trunk Untagged VLANs: n/a

Chapter 16 RMON

16.1 RMON principle interview

RMON is a standard of network data monitoring using different network Agent and manage station systems designated by IETF, which can make SNMP monitoring remote equipments more effectively and forwardly. Therefore, network administrator can track network, network segment and the equipment faults more quickly. This way reduces the data stream between the manage station and the Agent and makes simple and powerful management to large network, which makes up the limitation that SNMPS is facing in the distributed connection that is becoming larger and larger.

We can use SNMP Agent in the switch side to monitor and manage the switch network situation. Now the 1, 2, 3, 9 group of RMON is realized, that is statistic group, history group, alarm group and event group.

- ➢ Statistics: Collects Ethernet, Fast Ethernet, and Gigabit Ethernet statistics on an interface.
- ➢ History: Collects a history group of statistics on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces for a specified polling interval.
- ➢ Alarm: Monitors a specific management information base (MIB) object for a specified interval, triggers an alarm at a specified value (rising threshold), and resets the alarm at another value (falling threshold). Alarms can be used with events; the alarm triggers an event, which can generate a log entry or an SNMP trap.
- ➢ Event: Determines the action to take when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.

16.2   RMON configuration

16.2.1 Default RMON configuration

Function	Default value
Static group	Enabled
History static group	No
Alarm group	No
Event group	No

16.2.2 RMON static group configuration

Configure the port's statistic function parameter, if the port's statistic function is disabled, use the command to enable it again; if it is enabled, use the command to change the corresponding parameter. By default all the port's statistic function is enabled, use command **no** to disable it.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rmon statistics** {**ip** *l3_interface* | **port**	**ip** *l3_interface* set the statistics function of

		layer 3 interface, range is 0-14;
		port *port_list* set the statistics function for the physical port, range is 1-26;
		owner *STRING* set the owner name of current statistics group, default value is "monitorEtherStats".
3	**exit**	Exit from global configuration mode to enter privileged EXEC mode.
4	**show rmon statistics**	Show statistics group information.

To disable statistic group, use the command: **no rmon statistics {ip** *13_interface* | **port** *port_list}*

Notice：

> ➢ Before RMON function is configured, SNMP Agent correct configuration must be made sure.
> ➢ When the statistic function of some port is disabled, it means not that data statistic is stopped, but that user can no longer acquire the port's statistic data.

16.2.3 RMON history statistic and configuration

Configure the port's statistic function parameter. If the port's history statistic function is disabled, use the command to enable it again; if it is enabled, use the command to change the corresponding parameters. All the ports, including three-layer port and physical port, are open by default, Use command **no** to disable it. When one port's history group function is disabled, data collection and statistic function can not go on, and all the history data collected before will be cleared.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rmon history** {**ip***l3_interface* | **port** *port_list*} [**shortinterval** *short-time*] [**longinterval** *long-time*] [**buckets** *queuesize*] [**owner** *STRING*]	**ip** *l3_interface* Set the RMON history function of layer 3 interface, range is 0-14;
		port *port_list* set the RMON history function of physical port, range is 1-26;
		shortinterval *short-time:* the short time interval of history data collection of the port, range is 1-3600, default value is 2 seconds.
		longinterval *long-time* the long time interval of history data collection of the port, range is 1-3600, default value is 300 seconds (5 minutes);
		buckets *queuesize:* circular queue size for history data, range is 10-1000, default is 10.
		owner *STRING:* set the owner name of RMON history group, default name is "monitorHistory".
3	**exit**	Exit from global configuration mode and enter privileged EXEC mode.
4	**show rmon history**	Show history statistics information

16.2.4 RMON alarm group configuration

Use command **no** to delete a warning to configure a MIB variable that is being monitored,

The MIB variable that is being monitored must be really exist, and it must be INTEGER type in ASN.1 expression, like type of INTEGER, Counter, Gauge and TimeTicker. If the variable does not exist or the type is incorrect when configured, return fault; in the alarm that has been successfully configured, if the variable is not collected in the late time, the warning will be shut up. Re-configuration is needed to monitor the variable again.

If the index number of trigger event is not configured, the default value will be 0, which means the event will not be triggered, because 0 is not a valid event number. If the index number of the event is not 0, but the event is not configured correspondingly in the event group, then the event will not be triggered successfully when the monitoring variable exceeds until the event is established.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rmon event** *number* [**log**] [**trap**] [**description** *string*] [**owner** *string*]	*number* event index number **log** whether log the information and send system log information **trap** whether send trap **description** *string*: description string **owner** *string* the owner of the event
3	**exit**	Exit from global configuration mode.
4	**show event** *number*	Show configuration information

Use command **no alarm** *number* to delete alarm.

16.2.5 RMON event group configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rmon event** *number* [**log**] [**trap**] [**description** *string*] [**owner** *string*]	Configure the event group function parameter of the port. *number* event index number **description** *string* description character string **owner** *string* owner of the event
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show alarm** number	Show the configuration result number event index number

Use the command **no event** *number* to delete event.

16.2.6 Monitoring and maintenance

Command	Description
show rmon	Show all the RMON four group information
show rmon alarms	Show alarm information, including alarm number, name, threshold, sampling period and sampling value.
show rmon events	Show alarm information, including alarm number, name, threshold, sampling period and sampling value.
show rmon statistics	Show port information which has enabled statistics group.

Configure all the RMON groups' function to default state, that is the state when the switch has just been started

Step	Command	Description
1	**config**	Enter global configuration mode
2	**clear rmon**	Restore to the default state
3	exit	Quit global configuration mode and enter privileged EXEC mode.

16.2.7 Typical configuration example

1. Network requirement:

Agent connects the configuration terminal through console port, and connects remote NMS through Internet. In RMON Ethernet static table, set a table item, make performance statistic for Ethernet port, and record log when in a certain time the byte number that the port received exceeds the configured threshold.

2. Network figure
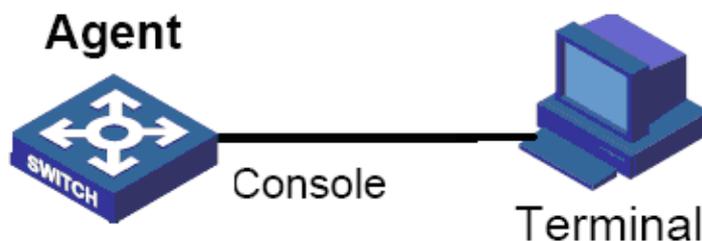
3. Configuration steps:

First, establish a event with the index number 1, and the description character stream is High-ifOutErrors for the event that sends out **log**, owner is system. Then, set a alarm, monitor MIB variable 1.3.6.1.2.1.2.2.1.20.1, examine if the variable is rising/falling every 20s, if it has rise 15, alarm will be triggered, the owner's name is the same with the event group.

Raisecom#**config**

Raisecom(config)#**rmon event** *1* **log description** *High-ifOutErrors* **owner system**

Raisecom(config)#**rmon alarm** *10* *1.3.6.1.2.1.2.2.1.20.1* **interval** *20* **delta rising-threshold** *15* *1* **falling-threshold** *0* **owner system**

Raisecom(config)#**exit**

Raisecom#**show rmon alarm**

Alarm 10 is active, owned by system

Monitors 1.3.6.1.2.1.2.2.1.20.1 every 20 seconds

Taking delta   samples, last value was 0

Rising threshold is 15, assigned to event 1

Falling threshold is 0, assigned to event 0

On startup enable rising and falling alarm

Raisecom#show rmon event

Event 1 is active, owned by system

Event generated at 0:0:0

Send TRAP when event is fired.

Chapter 17   ARP

This chapter is mainly about how to configure and maintain ARP on the switch, including:

✧   ARP interview
✧   ARP configuration
✧   Monitoring and maintenance
✧   Typical configuration example

17.1 ARP principle interview

When the switch software system is transmitting IP message, it is needed to look for its physical address according to the requirement so that the message can be sent to destination host. The mapping relationship of IP address and MAC address is kept in ARP address mapping table.

ARP address mapping table includes 2 types of MAC addresses:

➢   Dynamic learned MAC address: Dynamic MAC addresses learned through ARP protocol and will be aged if not used.
➢   Static MAC address: added manually to the table and do not age.

If host A sends IP packets to host B, host A uses the IP address of host B and searches corresponding MAC address in its own ARP table. If there is the MAC address of host B, host A will send the IP packet directly; if there is not the MAC address of host B , host A will send ARP request, get the MAC address of host B and add the address to the ARP table.

In most of the cases, when host A sends IP packets to host B, it is pretty possible that host B will sent packets to host A again, so host B will also need to send ARP request to host A. In order to reduce the traffic in the network, host A write its own MAC address in the ARP request. When host B receives the ARP request, it will record the MAC address of host A to its mapping table. Then it is more convenient for host B to communicate host A.

In some special situation, administrator also can configure ARP address mapping table manually.

17.2   ARP configuration

This part is about how to configure and maintain ARP on the switch, including:

➢   Default ARP configuration
➢   Adding stable ARP address table item
➢   Deleting ARP address mapping table item
➢   Configuring ARP dynamic address mapping table item overtime
➢   Configuring ARP dynamic learning mode
➢   Clearing ARP address mapping table

17.2.1 Default ARP configuration

Function	Default value
Stable ARP address table item	No
APR dynamic address mapping table item overtime	1200s
ARP dynamic learning mode	learn-reply-only

17.2.2 Adding dynamic ARP address table item

Usually, ARP mapping table is maintained by dynamic ARP protocol, ARP will search the resolution from IP address to MAC address according to the protocol, needing not the participation of administrator. Only when it is needed to add stable ARP table item will the ARP manual configuration commands be used to ARP mapping table.

Stable ARP address table item has the features below:

➢ Stable ARP address table item has to be added and deleted manually
➢ Stable ARP address will not grow old

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	**arp** *ip-address mac-address*	Add a stable table item to ARP address mapping table
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	show arp	Show all the table units in ARP address mapping table

Notice：The IP address that is stable added to ARP table item must belongs to the IP network segment that the switch's three-layer port belongs to.

Use global configuration command **no arp** *ip-address* to delete stable ARP table item.

17.2.3 Configure the overtime of ARP dynamic address table item

User can configure the existing time of ARP dynamic item, ARP dynamic table that exceeds the time will be deleted.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	**arp aging-time** *sec*	Configure the existing time of ARP dynamic table item, ARP dynamic table item that exceeds the time will be deleted
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	show arp	Show all the table items of ARP address mapping table

Notice: If the exceeding time is set to 0, ARP dynamic table item will no longer grow old.

Use global configuration command **no arp aging-time** to restore the default configuration of ARP dynamic address mapping table item exceeding time.

17.2.4 Configure ARP dynamic learning mode

It is mentioned above that, to reduce the network communication capacity, when host A is sending its ARP request group, it will write the mapping from its own IP address to the physical address into ARP request group. When host B receives the ARP request group from host A, host B will write the address mapping of host A into its own mapping table. This makes the process of host B sending data to host A more convenient. Configure ARP dynamic learning mode to realize the process mentioned above for learn-all.

The intention of configuring ARP dynamic learning mode is to prevent ARP attack from happening. When configured **learn-all** mode, the host will learn both ARP request message and response message; when configured **learn-reply-only** mode, it will learn ARP response message only, and responds ARP response messages only for request message, without learning ARP.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**arp mode** *{learn-all/ learn-reply-only}*	Configure ARP dynamic learning mode
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show arp**	Show all the table items in ARP address mapping table

17.2.5 Clearing ARP address mapping table

In some situations, network administrator may need to clear all the ARP table items. Use command **clear arp** to realize it.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**clear arp**	Clear all the table items in ARP address mapping table
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show arp**	Show all the table items in ARP address mapping table

17.3   Monitoring and maintenance

Use command **show arp** to show the commands of all the table items in the ARP address mapping table, including: the IP address of each table item, MAC address and table item type.

Command	Description
show arp	Show all the table items in ARP address mapping table

17.4   Typical configuration example

1) Network request:

- ➢ Configure the aging time of the switch dynamic ARP table item to 600s.
- ➢ To prevent ARP attack in some situations, configure the switch's dynamic ARP learning mode to **learn-reply-only.**
- ➢ Under the premise that IP port address is configured, add a stable ARP table item.

2) Configuration steps:

Raisecom(config)# **arp aging-time** *600*

Raisecom(config)# **arp mode learn-reply-only**

Raisecom(config)# **arp** *10.0.0.1 0050.8d4b.fd1e*

Chapter 18 SNMP

18.1SNMP principle

18.1.1 SNMP overview

Now, the network management protocol that is the most extensively used in computer network is SNMP (Simple Network Management Protocol), which is also one of the standard protocol for Internet management.

On structure, SNMP is made up of agent and Network Management Station (NMS), or agent/management station mode. Among them, NMS is the workstation that runs the client program, the management workstations that is usually used now are IBM NetView and Sun NetManager; Agent means the server software that is running on the network equipment like the switch, management information base （MIB） is maintained in Agent.

When SNMP Agent receives the request message Get-Request, Get-Next-Request, Get-Bulk-Request that about MIB variable from NMS, Agent will take read/write operation to the MIB variable that NMS requested according to the message type, then create Response message according to the result, and send it to NMS as response.

On the other side, when SNMP Agent receives the message about some equipment's state like cold/warm booting or anomalous event, it will create a Trap message and send it to NMS actively and report these important incidents.

Raisecom serious SNMP Agent supports SNMPv1, SNMPv2c and SNMPv3

18.1.2 SNMP V1/V2 interview

SNPMv1 is a simple request/response protocol. The network management system sends out a request, the manager returns a response. The action is realized by one of the four protocol operations. The four operations are GET, GETNEXT, SET and TRAP. Through GET operation, NMS get one or more object (instance) values. If the agent can not offer all the request (instance) values from the request list, it will not offer any value. NMS use GETNEXT operation to get the next object instance value from the request list or the object list. NMS use SET operation to send commands to SNMP proxy and request re-configuration to the object value. SNMP proxy use TRAP operation to inform NMS the specific event irregularly.

Different from SNMPv1's simplex centralized management, SNMPv2 supports distributed/layered network management structure, in SNMPv2 management model some systems have both manager and proxy function; as proxy, it can receive the commands from senior management system, interview the local information stored, and offer the information summary of other proxy in the management domain that it charges, then send Trap information to senior manager.

18.1.3 SNMPv3 interview

SNMPv3 uses user-based security model. Whatever it is NMS sending query message to SNMP Agent, or SNMP Agent sending Trap message to NMS, the communication between NMS and SNMP Agent must be

in the name of a certain user. Both SNMP NMS and proxy side maintains a local SNMP user table, user table record username, user related engine ID, if identification is needed and the identification key, encryption information, so that it could make correct resolution to the message content and suitable response. SNMP user's configuration is to create key through the password information in the command lines, and add a user in local SNMP user table of the switch.

18.2SNMPv1/v2/v3 management configuration

18.2.1 Default SNMP configuration

Function	Default value
trap switch	Enabled
The mapping relationship between SNMP user and visiting group	The existed ones by default: initialnone, initial group Index GroupName UserName SecModel 0 initialnone raisecomnone usm 1 initial raisecommd5nopriv usm 2 initial raisecomshanopriv usm
SNMP interview group	The existed ones by default: initialnone, initial group Index: 0 Group: initial Security Model: usm Security Level: authnopriv Context Prefix: -- Context Match: exact Read View: internet Write View: internet Notify View: internet Index: 1 Group: initialnone Security Model: usm Security Level: noauthnopriv Context Prefix: -- Context Match: exact Read View: system Write View: -- Notify View: interne
SNMP user	The existed ones by default: raisecomnone, raisecommd5nopriv, raisecomshanopriv user Index: 0 User Name: raisecomnone

	Security Name: raisecomnone
	EngineID: 800022b603000e5e00c8d9
	Authentication: NoAuth
	Privacy: NoPriv
	Index: 1
	User Name: raisecommd5nopriv
	Security Name: raisecommd5nopriv
	EngineID: 800022b603000e5e00c8d9
	Authentication: MD5
	Privacy: NoPriv
	Index: 2
	User Name: raisecomshanopriv
	Security Name: raisecomshanopriv
	EngineID: 800022b603000e5e00c8d9
	Authentication: SHA
	Privacy: NoPriv

SNMP group	The existed ones by default: public, private group			
	Index	Community Name	View Name	Permission
	1	public	internet	ro
	2	private	internet	rw

The network administrator's contact information and logo	Contact information: support@Raisecom.com
	Device location: world china raisecom
SNMP object host address	None
SNMP figure	The existed ones by default: system,internet figure
	Index: 0
	View Name: system
	OID Tree: 1.3.6.1.2.1.1
	Mask: --
	Type: included
	Index: 1
	View Name: internet
	OID Tree: 1.3.6
	Mask: --
	Type: included

18.2.2 SNMPv1/v2 configuration

To protect itself and keep MIB from invalid visit, SNMP Agent brings in the idea of group. The management station in a group must use the group's name in all the Get/Set operations, or the request will not be taken.

The group name uses different character stream to sign different SNMP groups. Different groups may have read-only or read-write visit right. The group that has read-only right can only query the equipment information, while the group with read-write right can not only query the equipment information but also configure it.

When SNMPv1 and SNMPv2 takes group name authentication project, the SNMP message whose group name is not accorded will be dropped. The whole configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
(optical)	**snmp-server view** *view-name oid-tree* [*mask*] {**included** | **excluded**}	Define the figure and the contained MIB tree range; *view-name:* figure name, the length can not exceed 32 character; *oid-tree:* 0ID tree, 0ID number which the depth can not exceed 128; *mask:* 0ID tree mask, the depth can not exceed 128, format is 0ID, each option of 0ID can be only 0 or 1;
2	**snmp-server community** *community-name* [**view** *view-name*] *{ro|rw}*	Configure the community name and the relevant attributes. *view-name:* the view name ro: read-only rw: read-and-write
3	**exit**	Return to privileged EXEC mode
4	**show snmp community**	Show group information

Notice：Both SNOMPv1 and SNMPv2 takes group name authentication project, the SNMP message that is not accord with the group name that has been identified will be dropped.

18.2.3 SNMPv3 configuration

SNMPv3 takes USM (user-based security model) which is based on user's security safety model. USM brings the principle of interview group: one user or several users accord with a interview group, each interview group set the corresponding write, read, notify view, the user in interview group has the right in the figure. The interview group in which user send requests likeGet and Set must have the corresponding right, or the request will not be taken.
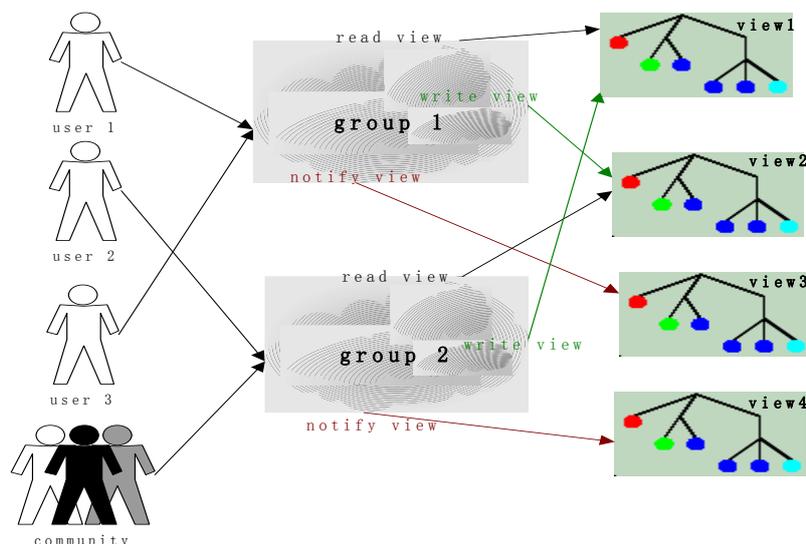
From the figure above, we can see that the normal interview to the switch for NMS, needs not only configuring the user but also making sure which group the user belongs to, the figure right that the interview group has and each figure. Complete configuration (including user's configuration) process is as follow:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server user** *username* [**remote** *engineid*] [**authentication**{**md5** | **sha**} *authpassword*]	Add a user
3	**snmp-server view** *view-name oid-tree* [*mask*] {**included** | **excluded**}	Define the view and its privilege of the MIB *view-name* specify the configured name of view ,*oid-tree* specify OID tree *mask* the mask of OID sub-tree, each bit corresponds to a note of the sub-tree **included** means that the scale of the view includes all the MIB variables under OID tree **excluded** means that the scale of the view includes all the MIB variables out of OID tree
4	**snmp-server group** *groupname* **user** *username* { **v1sm** | **v2csm** | **usm**}	Configure the group which the user belongs to
5	**snmp-server access** *groupname* [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**context** *contextname* [{**exact** | **prefix**}]] { **v1sm** | **v2csm** | **usm**} { **noauthnopriv** | **authnopriv** }	Define the access privilege of the group *Groupname* is the name of access group; *readview* is the read view, default is internet; *writeview* is the write view, default is empty; *notifyview* is informational view, default is empty; *contextname* is the name of context or its prefix; **exact|prefix** stands for the match type of the context name: **exact** means the input should be fully matched with the name of context, **prefix** means that only the first several letters should match with the name of context;

		v1sm|v2csm|usm are the security model, stands for SNMPv1 security model,SNMPv2 is the security model based on community and SNMPv3 is the security model based on the user respectively;
		noauthnopriv|authnopriv is the security level, stands for no authentication and no encryption, or authentication without encryption respectively.
6	**exit**	Exit to privileged configuration mode
7	**show snmp group** **show snmp access** **show snmp view** **show snmp user**	Show SNMP configuration information

18.2.4 SNMP v1/v2 TRAP configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** 0	Enter IP port mode
3	**ip address** A.B.C.D[A.B.C.D] vlanID	Configure the switch IP address A. B. C. D IP address [A. B. C. D] subnet mask vlanID vlan number
4	**exit**	Quit global configuration mode and enter privileged EXEC mode
5	**snmp-server host** *A.B.C.D* **version** {**1|2c**} NAME [**udpport** *<1-65535>*] [**bridge**] [**config**] [**interface**] [**rmon**] [**snmp**] [**ospf**]	Configure SNMPv1/v2 Trap object host A.B.C.D NMS IP address NAME SNMPv1/v2c group name *<1-65535>* receiving port number that object host receives Trap, by default it is 162;
6	**exit**	Return to privileged EXEC mode
7	**show snmp host**	Show configuration state

18.2.5 SNMPv3 Trap configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** *0*	Enter IP port mode
3	**ip address** *A.B.C.D [A.B.C.D] vlanID*	Configure the switch IP address

		A.B.C.D: IP address
		[A.B.C.D]: subnet mask
		vlanID: vlan number
4	**exit**	Quit global configuration mode and enter privileged EXEC mode
		Configure SNMPv3 Trap object host
5	**snmp-server host** *A.B.C.D* **version** 3 { **noauthnopriv** | **authnopriv** } NAME [**udpport** *<1-65535>*] [**bridge**] [**config**] [**interface**] [**rmon**] [**snmp**] [**ospf**]	*A.B.C.D*: HOST IP address
		NAME: SNMPv3 username
		<1-65535>: receiving port number that object host receives Trap, by default it is 162;
6	**exit**	Return to privileged EXEC mode
7	**show snmp host**	Show configuration state

18.2.6 Other SNMP configuration

1. Configure the network administrator label and contact access

The network administrator label and contact access sysContact is a variable of system group, its effect is to configure the network administrator label and contact access for management switch.

Step	Command	Description
1	**config**	Enter global configuration
2	**snmp-server contact** *sysContact*	Configure network administrator label and contact access
3	**exit**	Return to privileged EXEC mode
4	**show snmp config**	Show configuration situation

2. Enable/disable system sending trap message

Trap is used mainly for providing some switch important events to NMS. For example, when receiving a request with a fault group name and being allowed to send SNMP Trap, the switch will send a Trap message of failed authentication.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server enable traps**	Allow the switch to send trap
3	**exit**	Return to privileged EXEC mode
4	**show snmp config**	Show the configuration

Use command **no snmp-server enable traps** to stop the switch from sending trap.

3. Configure the switch position

The switch position information sysLocation is a variable of MIB system group, which is used to describe the physical position of the switch.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server location** *sysLocation*	Configure the switch position *sysLocation:* specify the switch physical position, the type is character stream
3	**exit**	Return to privileged EXEC mode
4	**show snmp config**	Show the configuration

18.2.7 Monitoring and maintenance

Step	Command	Description
1	**show snmp community**	Show SNMP community information
2	**show snmp host**	Show IP address of trap target host computer.
3	**show snmp config**	Show the SNMP engine ID, network administrator contact method, the position of the switch and whether TRAP is enabled.
4	**show snmp view**	Show view information
5	**show snmp access**	Show all the names of access group and the attributes of access group.
6	**show snmp group**	Show all the mapping relationship from user to access group.
7	**show snmp user**	Show the user information, authentication and encryption information.
8	**show snmp statistics**	Show SNMP statistics information

18.2.8 Typical configuration example

The interview control configuration example of V3:
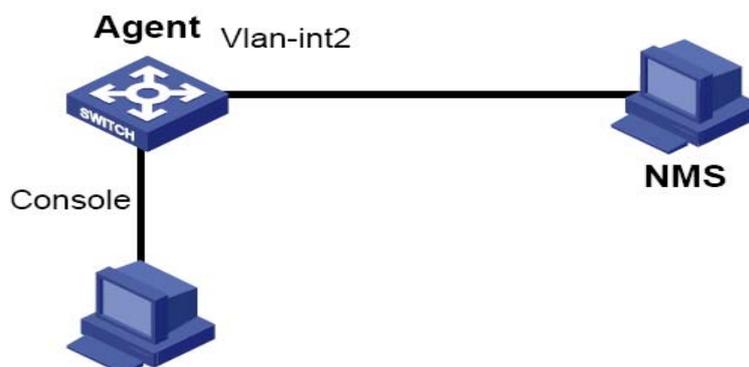
First, set the local switch IP address to 20.0.0.10, user *guestuser1*, uses md5 identification algorithm, with the identification password raisecom, to interview the figure of MIB2, including all the MIB variable under

1.3.6.1.x.1, create guestgroup interview group, the safe mode safe model is usm, the safe grade is identified but not encrypted, the readable figure name is MIB2, thus the process of *guestuser1* mapping to interview group with the safe grade usm can be accomplished, and the result will be shown:

Raisecom#**config**

Raisecom(config)# **interface ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**snmp-server view** *mib2 1.3.6.1.2.1   1.1.1.1.0.1* **included**

    Set successfully

Raisecom(config)#**snmp-server user** *guestuser1* **authentication md5** *raisecom*

    Set successfully

Raisecom(config)#**snmp-server access** *guestgroup* **read** *mib2* **usm authnopriv**

    Set successfully

Raisecom(config)#**snmp-server** group *guestgroup* **user** *guestuser1* **usm**

    Set successfully

Raisecom(config)#**exit**

Raisecom# **show snmp access**

  Index: 0

  Group: initial

  Security Model: usm

  Security Level: authnopriv

  Context Prefix: --

  Context Match: exact

  Read View: internet

  Write View: internet

  Notify View: internet

  Index: 1

  Group: guestgroup

  Security Model: usm

  Security Level: authnopriv

  Context Prefix: --

  Context Match: exact

  Read View: mib2

  Write View: --

  Notify View: internet

  Index: 2

Group: initialnone

Security Model: usm

Security Level: noauthnopriv

Context Prefix: --

Context Match: exact

Read View: system

Write View: --

Notify View: internet

Raisecom# **show snmp group**

Index	*GroupName*	*UserName*	*SecModel*
0	*guestgroup*	*guestuser1*	*usm*
1	*initialnone*	*raisecomnone*	*usm*
2	*initial*	*raisecommd5nopriv*	*usm*
3	*initial*	*raisecomshanopriv*	*usm*

V3 Trap configuration example:

Trap is the information Agent sending to NMS actively, used to report some urgent events. As is shown below, set the switch IP address to 20.0.0.10, NMS host IP address to 20.0.0.221, username to raisecom, SNMP version v3, identified but not encrypted, all Trap
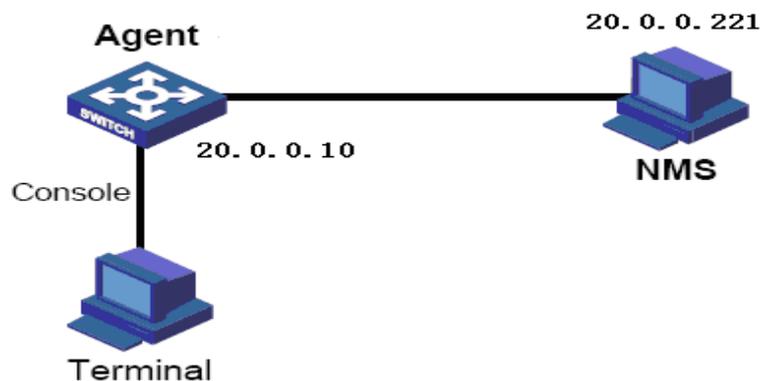
Raisecom#**config**

Raisecom(config)# **int ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**snmp-server host** *20.0.0.221* **version** *3* authnopriv   *raisecom*

Raisecom#**show snmp host**

Index: 0

IP address: 20.0.0.221

Port: 162

User Name: raisecom

SNMP Version: v3

Security Level: authnopriv

TagList: bridge config interface rmon snmp ospf

Chapter 19   Cluster Management

19.1 Cluster management introduction

19.1.1 Cluster definition

Using cluster management function, network administrator can manage several switches through the public IP address of a main switch. The main switch will be command equipment, while other switches under administration will be member equipments. The member equipment will not be configured IP address usually, use management equipment redirection to manage and maintain the member equipments.

19.1.2 Cluster role

The position and function of the switch are different in the cluster, so different switch has different role in the cluster. The switches can be commander, member and candidate.

- ➤ Commander equipment: the commander has public IP address, provides the management interface for all the switches in the cluster. Commander uses command redirection to manage the members: users send the management command to the commander through public network, and the commander will handle the command, if the commander finds that this command is for other members it will send the commands to members. Commanders have the functions: discover neighbor Raisecom switches, collect the network topology, cluster management, maintaining cluster status, and support different proxy.
- ➤ Member equipment: cluster members do not have IP address. User uses the command redirection function to manage the device. Member device has the functions including discovering neighbor, receiving the management info of commander, executing the proxy command, failure/log report function. Once the member is active, it can be managed by network commander.
- ➤ Candidate equipment: the switch does not join any cluster but do have cluster capability, it can be member.

19.1.3 Cluster principle

There are three main cluster protocols: RNDP (Raisecom Neighbor Discover Protocol), RTDP (Raisecom Topology Discover Protocol) and RCMP (Raisecom Cluster Management Protocol). RNDP is in charge of neighbor discovery and information collection, RTDP is in charge of the collecting and processing topology information, RCMP is in charge of the functions like adding, active, and deleting cluster members. RTDP and RCMP protocol communicate with each other in VLAN 2. So if there is no such a device that supports Raisecom cluster management functions between two cluster management devices. It needs proper configuration for VLAN2 to make sure normal communication between RTDP and RCMP.

Each cluster has to designate a commander. When commander is designated, it can discover candidates by RNDP and RTDP.

When candidate is added to the cluster, it becomes a member; user has to active this switch by cluster management function, or by configuring automatically active function on the switch to active the cluster function.

19.2   Configure RNDP function

19.2.1 Default RNDP function configuration

By default, the command configuration is as follows:

Function	Default configuration
Enable/disable global RNDP function	Enable the switch RNDP and all the port's RNDP

19.2.2 Configure RNDP function

19.2.2.1   Enable global RNDP

In global configuration mode enable or disable global RNDP function, by default the system RNDP function is enabled, all the ports take part in RNDP judgment and discovery.

Step	Command	Description
1	config	Enter global configuration mode
2	rndp *{enable | disable}*	Enable/disable RNDP globally
3	exit	Return to privileged EXEC mode
4	show rndp	Show RNDP configuration

19.2.2.2   Enable RNDPP port

To enable/disable port RNDP function in port configuration mode, by default all the ports take part in RNDP judgment and discovery.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port *<1-26>*	Enter port configuration mode
3	rndp *{enable | disable}*	Enable/disable port RNDP
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show rndp	Show RNDP configuration

19.2.3 Monitoring and maintenance

Use command **show** to monitor and maintain RNDP.

Command	Description
show rndp	Show RNDP configuration information
show rndp neighbor	Show RNDP neighbor information

19.2.4 Typical configuration example

Topology structure is as follows:
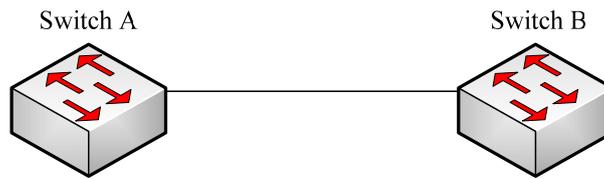
Fig 1 topology structure

As is shown in figure 1, connect SwitchA and SwitchB, enable all the ports RNDP for SwitchA, enable all the ports RNDP for SwitchB.

SwtichA configuration is show below:

Raisecom#**config**

Raisecom(config)#**interface range** *1-26*

Raisecom(config-range)#**rndp** *enable*

Raisecom(config-range)#**exit**

Raisecom(config)#**exit**

Raisecom#**show rndp**

Raisecom#**show rndp neighbor**

  Global RNDP feature: Enabled

  Participant ports: 1-26

  MAC Address   LocalPort RemotePort SysID   Hostname

  000E.5E03.5318   6   4   6001E   ISCOM2926

SwitchB configuration is as follows:

Raisecom#**config**

Raisecom(config)# **rndp** *enable*

Raisecom(config)#**interface range** *1-26*

Raisecom(config-range)#**rndp** *enable*

Raisecom(config-range)#**exit**

Raisecom(config)#**exit**

Raisecom#**show rndp**

Raisecom #**show rndp neighbor**

  Global RNDP feature: Enabled

  Participant ports: n/a

MAC Address	LocalPort	RemotePort	SysID	Hostname
000E.5E00.C8D9	4	6	60002	ISCOM3026

19.3 RTDP function configuration

19.3.1 Default RTDP function configuration

By default, the command configuration is as follows:

Function	Default configuration
Enable/disable RTDP collection function	Disabled
RTDP collection range	The maximum RTDP collection range is 16 hop.

19.3.2 RTDP function configuration

19.3.2.1 Enable RTDP

Under global configuration mode, user can enable or disable RTDP function, RTDP is disabled by default. If RTDP is enabled, RTDP will collect all the information of Raisecom switch which RNDP function is enabled.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rtdp** *{enable | disable}*	Enable or disable RTDP collection.
3	**exit**	Exit to privilege EXEC mode.
4	**show rtdp**	Show RTDP collection.

19.3.2.2 RTDP collection range

In global configuration mode, configure RTDP collection range, by default RTDP can collect the equipment information within 16 hop.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rtdp max-hop** *<1-16>*	Configure RTDP collection range
3	**exit**	Return to privileged EXEC mode
4	**show rtdp**	Show RTDP configuration

19.3.3 Monitoring and maintenance

Use command **use** to monitor and maintain RTDP.

Command	Description

show rtdp	Show RTDP configuration information
show rtdp device-list [*HHHH.HHHH.HHH* | *hostname*] [**detailed**]	Show RTDP discovery equipment list information

19.3.4 Typical configuration example

The topology structure is shown below:
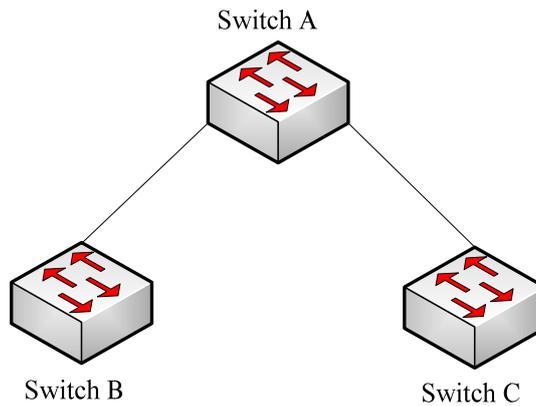
Fig 2 topology structure

As is shown in figure 2, connect the port of SwitchA with the port of SwitchB and SwitchC respectively, on SwitchA configure RTDP enabled and the collection range to 3, configure SwitchB to RTDP enabled, SwtichC to RTDP disabled.

SwitchA configuration is as follows:

Raisecom#**config**

Raisecom(config)#**rtdp** *enable*

Raisecom(config)#**rtdp max-hop** *3*

Raisecom(config) #**exit**

Raisecom #**show rtdp**

Raisecom#**show rtdp device-list detailed**

RTDP max-hop: 3

RTDP collecting feature: Enabled

RTDP reporting feature: Enabled

MAC Address   RcvdPort   Hop   SysID   Hostname

--

000E.5EBD.5951   8   1   60011   ISCOM2009

  -Device cluster information:

    Idendity: Candidate

    Autoactive: Disabled

  -Device adjacency information:

Mac Address   LocalPort   RemotePort

000E.5E00.C8D9   8   2

--

000E.5E03.5318   6   1   6001E   ISCOM2926

  -Device cluster information:

    Idendity: Candidate

    Autoactive: Disabled

  -Device adjacency information:

    Mac Address   LocalPort   RemotePort

    000E.5E00.C8D9   6   4

--

SwitchB configuration is as follows:

Raisecom#**config**

Raisecom(config)#**rtdp** *enable*

Raisecom(config) #**exit**

Raisecom #**show rtdp**

Raisecom#**show rtdp device-list detailed**

    RTDP max-hop: 16

    RTDP collecting feature: Enabled

    RTDP reporting feature: Enabled

    MAC Address   RcvdPort   Hop   SysID   Hostname

    --

    000E.5EBD.5951   4   2   60011   ISCOM2009

      -Device cluster information:

        Idendity: Candidate

        Autoactive: Disabled

      -Device adjacency information:

        Mac Address   LocalPort   RemotePort

        000E.5E00.C8D9   8   2

    --

000E.5E00.C8D9   4   1   60002   ISCOM3026

   -Device cluster information:

    Idendity: Candidate

    Autoactive: Disabled

  -Device adjacency information:

  Mac Address   LocalPort   RemotePort

  000E.5E03.5318   4   6

  000E.5EBD.5951   8   2

  --

SwitchC configuration is as follows:

Raisecom#**config**

Raisecom(config)#**rtdp** *disable*

Raisecom(config) #**exit**

Raisecom #**show rtdp**

  RTDP max-hop: 16

  RTDP collecting feature: Disabled

  RTDP reporting feature: Enabled

19.4   Cluster management function configuration

19.4.1 Default cluster management function configuration

Command	Default configuration
Disable or enable cluster management	Disable cluster management function
Disable or enable cluster management	Automatically active function disabled
Configure the MAC address of automatically active command switch	Default configuration is 0000.0000.0000.

19.4.2 Cluster management equipment function configuration

19.4.2.1 Enable/disable cluster management

By default system cluster management is disabled. With the steps below user can disable/enable cluster management, the command is used in the switch that has been command device.

Step	Command	Description

1	**config**	Enter global configuration mode
2	**cluster**	Enable cluster management function
3	**exit**	Return to global configuration mode
4	**exit**	Return to privileged EXEC mode
5	**show cluster**	Show cluster related information

19.4.2.2 Enable automatically active function

By using automatically active function and the configuring MAC address of the command switch that automatically active belongs to, when the equipment has connected to the network, it can be activated by the command switch it belongs to automatically. By default the system automatically active function is disabled. Follow the steps below to enable or disable automatically active function:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**[no] cluster-autoactive**	Disable/enable automatically active function
3	**[no] cluster-autoactive commander-mac** *HHHH.HHHH.HHHH*	Configure the MAC address of the command switch that automatically function belongs to
4	**exit**	Return to privileged EXEC mode
5	**show cluster**	Show cluster related information

19.4.3 Cluster member equipment function configuration

Add and active all the candidate member

For the convenience of user add and active operation to cluster member, the command allows user to use the same username and password to add & active, or add and active all the candidate members that is configured automatically active function by the command switch, and add & active all the candidate member one by one driven by commands.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**cluster**	Enter cluster management mode
3	**member auto-build** [{**active** *username password*}| {**active** *username password* **all**}]	Add all the candidate member; Active means activate all the candidate members; Username activated user's uername; Password activated user's password; All add and activate all the members
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show cluster member**	Show cluster member related information.

Notice: Automatically add and activate all the candidate members that are configured activated by current command switch, the members can use command **member auto-build**. With the command, use **member**

auto-build active *username password* to add and activate all the candidate members one by one. Use command **member auto-build active** *username password* **all.**

19.4.4 Add and activate cluster member

In cluster management mode, user can add the equipment that needs cluster management and activate it. When the equipment is added into the cluster but not activated, it can not manage the equipment the equipment through cluster management function. User can follow the steps below to add member to the cluster and activate it.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**cluster**	Enter cluster management mode
3	**member** *HHHH.HHHH.HHHH* **active** [*username password*]	Add a candidate member to the cluster; Active: activate the added equipment Username: activate the username that the equipment uses; Password: the password that is used to activated the quipment;
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show cluster member** [*HHHH.HHHH.HHHH*]	Show cluster member related information

19.4.5 Delete and suspend cluster member

19.4.5.1 Delete cluster member

In cluster management mode, user can delete the equipment that needs not cluster management. Follow the steps below to delete cluster member:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**cluster**	Enter cluster management mode.
3	**no member** {*HHHH.HHHH.HHHH*|**all**}	Delete one or all the members; HHHH.HHHH.HHHH: the member's MAC address that will be deleted. All: delete all the members;
4	**exit**	Exit to global configuration mode.
5	**exit**	Exit to privilege EXEC mode
6	**show cluster member**	Show cluster member information

19.4.5.2 Suspend cluster member

In cluster management mode, user can suspend the member which is in active mode, but it has not been deleted from the cluster. When the device is suspended, user cannot manage the device by cluster management any more. Follow the steps below to active cluster member:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**cluster**	Enter cluster management mode
3	**member** *HHHH.HHHH.HHHH* **suspend**	Suspend cluster member. *HHHH.HHHH.HHHH*: stands for the MAC address of the device that will be suspended. Suspend is the key word to be suspended.
4	**exit**	Exit to global configuration mode.
5	**exit**	Exit to privilege EXEC mode.
6	**show cluster member**	Show cluster member information.

19.4.6 Cluster member remote access

In cluster management mode, user can remotely manage the members which have been active, refer following commands:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**cluster**	Enter cluster management mode
3	**rcommand** {*hostname*| *HHHH.HHHH.HHHH*}	Login cluster member, the hostname is the member name, HHHH.HHHH.HHHH is the MAC address of the member.

19.4.7 Monitoring and maintenance

Use command **show** to realize the monitoring and maintenance of cluster management function.

Step	Command	Description
1	**show cluster**	Show cluster information
2	**show cluster member** [*HHHH.HHHH.HHHH*]	Show cluster member information
3	**Show cluster candidate**	Show cluster candidate information

Use show cluster to check current cluster relevant information:

Raisecom# **show cluster**

Use **show cluster member** [HHHH.HHHH.HHHH] to check particular cluster member or all the member information:

Raisecom# **show cluster member**

Use **show cluster candidate** to check candidates' information:

Raisecom# **show cluster candidate**

19.4.8   Typical configuration example

The topology structure is shown below:

Switch A
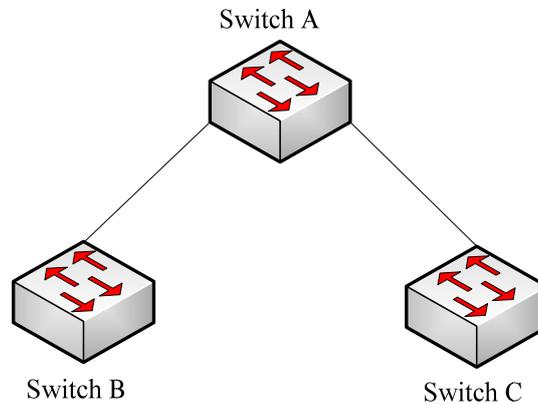
Switch B   Switch C

Fig 3 topology structure

As is shown in figure 3, SwitchA is set to cluster manager, SwitchB and SwitchC are added to cluster member. User can land to SwtichB and SwtichC on Switch.

SwitchA configuration is as follows:

Raisecom#**config**

Raisecom(config)#**rndp** *enable*

Raisecom(config)#**interface range** *1-26*

Raisecom(config-range)#**rndp** *enable*

Raisecom(config-range)#**exit**

Raisecom(config)#**rtdp** *enable*

Raisecom(config)#**cluster-autoactive**

Raisecom (config)#**cluster**

Raisecom (config-cluster)# **member auto-build active all** *raisecom*

Raisecom (config-cluster)#**exit**

Raisecom(config)#**exit**

Raisecom #**show cluster**

Raisecom#**show cluster member**

    Identity:Commander

    Current member number:2

    Max member number:128

    MAC Address   *Operation*   *State*   *Hostname*

```
-----------------------------------------------------
000E.5EBD.5951    Up              Active        ISCOM2009

000E.5E03.023C    Up              Active        IS2926-53
```

SwitchB configuration is as follows:

Raisecom#**config**

Raisecom(config)#**rndp** *enable*

Raisecom(config)#**interface range** *1-26*

Raisecom(config-range)#**rndp** *enable*

Raisecom(config-range)#**exit**

Raisecom(config)#**rtdp** *enable*

Raisecom(config)#**cluster-autoactive**

Raisecom(config)#**cluster-autoactive commander-mac** *000e.5e03.5318*

Raisecom(config)#**exit**

Raisecom #**show cluster**

 Identity:Member

 Autoactive:ON

 Autoactive commander mac:000e.5e03.5318

 Commander mac:000e.5e03.5318

SwitchC configuration is as follows:

Raisecom#**config**

Raisecom(config)#**rndp** *enable*

Raisecom(config)#**interface range** *1-9*

Raisecom(config-range)#**rndp** *enable*

Raisecom(config-range)#**exit**

Raisecom(config)#**rtdp** *enable*

Raisecom(config)#**cluster-autoactive**

Raisecom(config)#**cluster-autoactive commander-mac** *000e.5e03.5318*

Raisecom(config)#**exit**

Raisecom #**show cluster**

 Identity:Member

 Autoactive:ON

 Autoactive commander mac:000e.5e03.5318

 Commander mac:000e.5e03.5318

SwitchA loading to SwitchB:

Raisecom#**config**

Raisecom(config)#**cluster**

Raisecom(config-cluster)# **rcommand** *ISCOM2009*

    *Login:**raisecom***

    Password:

    Hello, Welcome to Raisecom Switch Operating System(ROS) software .

    Copyright (c) 2004-2006 Raisecom Technology Co., Ltd .

    ISCOM2009>**enable**

    Password:

ISCOM2009#**show cluster**

    Identity:Member

    Autoactive:ON

    Autoactive commander mac:000e.5e03.5318

    Commander mac:000e.5e03.5318

ISCOM2009#**exit**

Connection to host lost.

Chapter 20　System Log

20.1 System log function introduction n

20.1.1 System log function overview

The switch system information and some debugging output will be sent out for log handling, which will decide the destination that the log information will be sent according to the system log configuration: log files, console, TELNET, log host.

20.1.2 System log format

The format of system log is:

timestamp　module-level- Message content

For example: FEB-22-2005 14:27:33 CONFIG-7-CONFIG: USER "raisecom" Run "logging on".

20.2　　Configure system log function

20.2.1　Default system log configuration

Function	Default value
Set the log information to export to the console	Console the direction of the log host is enabled; Output scale is informational。
Set the log information to export to file	Enable the output of the log on file direction
Configure log host	The configuration information without log host
Configure the log exporting to monitor	Monitor the direction of log host is disabled
Enable/disable system log	Enable
Log rate configuration	The sending rate without the limit of logs
Configure the time stand of the log information	Use standard time

20.2.2 Configure system log source

20.2.2.1　Enable/disable system log

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging on**	Enable system log
3	**exit**	Return to privileged EXEC mode

	4	show logging	Show the configuration

For example:

Raisecom#**config**

Configuration mode, one conmmand input per times. End with CTRL-Z.

CONFIG-I:Configured from console ...

Raisecom(config)#**logging on**

set successfully!

Raisecom(config)#**exit**

Raisecom#**show logging**

Syslog logging:Enable, 0 messages dropped, messages rate-limited 0 per second

Console logging:Enable, level=informational, 0 Messages logged

Monitor logging:Disable, level=informational, 0 Messages logged

Time-stamp logging messages: date-time

Log host information:

Target Address	*Level*	*Facility*	*Sent*	*Drop*

20.2.2.2 Configure the time stand of the log information

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging time-stamp** *{standard|relative-start|null}*	Time stamp setting
		standard: standardtime mmm-dd-yyyy hh-mm-ss, for example "FEB-22-2005 14:27:33"
		relative-start: switch running time hh-mm-ss, for example "29:40:6" means the switch has been running for 29 hours 40 minutes 6 second
		null: no time stamp in log information
3	**exit**	Back to privileged EXEC mode
4	**show logging**	View the configuration

For example:

Raisecom#**config**

Raisecom(config)#**logging time-stamp relative-start**

20.2.2.3　Configure the log rate

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging rate** *<1-1000>*	Configure the log number sent every second
3	**exit**	Return to privileged EXEC mode

20.2.3　Configure system log output

20.2.3.1　Log information output to console

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging console** *{<0-7>| alerts|critical|debugging| emergencies|errors|informational |notifications|warnings}* **no logging console**	Configure and enable log information output to console and the parameter information, use command **no** to close the log output direction <0-7>log scale alerts　immediate action is needed (scale 1) critical critical state (scale 2) Debugging debug the information (scale 7) emergencies system not available (scale 0) errors errors (scale 3) Informational inform the event (scale 6) notifications　normal event in the critical condition (scale 5) Warnings warning condition (scale 4)
3	**exit**	Return to privileged EXEC mode
4	**show logging**	Show the configuration

20.2.3.2　Configure the log host

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging host** *A.B.C.D {local0 |local1|local2|local3|local4 |local5|local6|local7} {<0-7>| alerts|critical|debugging| emergencies|errors| informational|notifications|war nings}* **no logging host** *A.B.C.D*	Configure and enable log information output to console and the parameter information, use command **no** to close the log output direction. Local0-local7 the name of log host equipment <0-7>log scale alerts　immediate action is needed (scale 1) critical critical state (scale 2)

		Debugging debug the information (scale 7)
		emergencies system not available (scale 0)
		errors errors (scale 3)
		Informational inform the event (scale 6)
		notifications normal event in the critical condition (scale 5)
		Warnings warning condition (scale 4)
3	**exit**	Return to privileged EXEC mode
4	**show logging**	Show the configuration

20.2.3.3   Configure the log information to the file

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging file** **no logging file**	Configure and start recording the log information into flash files, use command **no** to close the log output direction
3	**exit**	Return to privileged EXEC mode
4	**show logging**	Show the configuration

20.2.3.4   Configure the log output to monitor

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging monitor** *{<0-7>|alerts|critical|* *debugging|emergencies|errors|* *informational|notifications|* *warnings}* **no logging monitor**	Configure and enable log information output to console and the parameter information, use command **no** to close the log output direction *<0-7>*:log scale *alerts*: immediate action is needed (scale 1) *critical*: critical state (scale 2) *debugging*: debug the information (scale 7) *emergencies*: system not available (scale 0) *errors*: errors (scale 3) *informational*: inform the event (scale 6) *notifications*: normal event in the critical condition (scale 5) *warnings*: warning condition (scale 4)
3	**exit**	Return to privileged EXEC mode
4	**show logging**	Show the configuration

20.2.4 Monitoring and Maintenance

Use command **show** to monitor and maintain log function

Command	Description
show logging	Show the configuration
show logging file	Show the log file content

For example:

Use **show logging** to look over the current log configuration state:

Raisecom# **show logging**

> *Syslog logging:Enable, 0 messages dropped, messages rate-limited 0 per second*
>
> *Console logging:Enable, level=informational, 0 Messages logged*
>
> *Monitor logging:Disable, level=informational, 0 Messages logged*
>
> *Time-stamp logging messages: date-time*

Log host information:

Target Address	Level	Facility	Sent	Drop

Use **show logging file** to look over the log file content:

Raisecom# **show logging file**

> *0:15:44   CONFIG-7-REBOOT-A:Reboot system by raisecom*
>
> *0:15:43   CONFIG-7-CONFIG:USER "raisecom"   Run "erase"*
>
> *0:15:43   CONFIG-7-ERASE-A:Erase system configuration file by raisecom*
>
> *0:15:31   CONFIG-6-LINK_U:port 24 Link   UP*
>
> *0:11:6   CONFIG-6-LINK_U:port 17 Link   UP*
>
> *0:11:4   CONFIG-6-LINK_D:port 17 Link Down*
>
> *0:10:40   CONFIG-6-LINK_D:port 24 Link Down*
>
> *0:10:39   CONFIG-6-LINK_U:port 17 Link   UP*
>
> *0:10:37   CONFIG-6-LINK_D:port 17 Link Down*
>
> *0:10:33   CONFIG-6-LINK_U:port 17 Link   UP*
>
> *0:10:30   CONFIG-6-LINK_D:port 17 Link Down*
>
> *0:10:29   CONFIG-6-LINK_U:port 17 Link   UP*
>
> *0:7:4   CONFIG-6-LINK_U:port 24 Link   UP*
>
> *0:3:6   CONFIG-7-LOGIN-A:user: raisecom Login*

20.2.5 Typical configuration example

Topology structure:

Fig 1 Topology structure

As is shown in fig 1, configure the switch IP address to 20.0.0.6, then start logging function, configure logging host, configure the IP address to 20.0.0.168.

The switch configuration is as follows:

Raisecom#**config**

Raisecom(config)# **interface ip** *0*

Raisecom(config-ip)# **ip address** *20.0.0.6 255.0.0.0 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**logging on**

Raisecom(config)#**logging time-stamp date-time**

Raisecom(config)#**logging rate** *2*

Raisecom(config)#**logging host** *20.0.0.168 local0 warings*

Raisecom(config)#**exit**

Raisecom#**show logging**

Syslog logging:Enable, 0 messages dropped, messages rate-limited 2 per second

Console logging:Enable, level=informational, 16 Messages logged

Monitor logging:Disable, level=informational, 0 Messages logged

Time-stamp logging messages: date-time

Log host information:

Target Address	Level	Facility	Sent	Drop
20. 0. 0.168	warnings	local0	11	0

PC show logging file:

07-01-200811:31:28   Local0.Debug   20.0.0.6   JAN   01   10:22:15   ISCOM3026:   CONFIG-7-CONFIG:USER "raisecom"   Run "logging on"

07-01-200811:27:41   Local0.Debug   20.0.0.6   JAN   01   10:18:30   ISCOM3026:   CONFIG-7-CONFIG:USER "raisecom"   Run "ip address 20.0.0.6 255.0.0.0 1"

07-01-200811:27:35   Local0.Debug   20.0.0.10   JAN   01   10:18:24   ISCOM3026:   CONFIG-7-CONFIG:USER "raisecom"   Run "ip address 20.0.0.6 255.0.0.1 1"

07-01-200811:12:43   Local0.Debug   20.0.0.10   JAN   01   10:03:41   ISCOM3026:   CONFIG-7-CONFIG:USER

"raisecom"   Run "logging host 20.0.0.168 local0 7"

07-01-200811:12:37   Local0.Debug   20.0.0.10   JAN   01   10:03:35   ISCOM3026:   CONFIG-7-CONFIG:USER "raisecom"   Run "logging on"

Chapter 21　System Clock Management

21.1 System clock management overview

Raisecom offers two ways for configuring system time: first, use SNTP protocol to make the switch system time accord with SNMP host time, configure the SNMP protocol time for synchronization to Greenwich time, and turn it to local time according to the system time zone configuration; second, configure the system time manually to local time.

21.2　System clock configuration function

21.2.1 Default system clock configuration

Function	Default value
Default time	2000-01-01　08:00:00
Default time zone excursion	+08:00
Default summer time function	Disable

21.2.2 Configure system clock function

Step	Command	Description
1	**clock set** *<1-24> <0-60> <0-60> <2000-2199> <1-12> <1-31>*	Configure system time, in turn they are: hour, minute, second, year, month, day
2	**show clock**	Show the configuration

21.2.3 Configure time zone management function

Step	Command	Description
1	**show clock**	Show the configuration
2	**clock set** *<1-24> <0-60> <0-60> <2000-2199> <1-12> <1-31>*	Configure system time, in turn they are: hour, minute, second, year, month, day
3	**clock timezone** *{+/-} <0-11> <0-59>*	Configure system time zone: +: eastern hemisphere -: western hemisphere *<0-11>* : time zone excursion, hour *<0-59>*: time zone excursion, hour

		By default it is Beijing time, that is eastern hemisphere 8h whole.

21.2.4 Configure summer time function

When summer time configuration is enabled, the time that is accord with SNMP will be transformed into local summer time. The steps are as follows:

Step	Command	Description
1	**clock summer-time enable**	Enable the summer time function. This function can also be shutdown if you do not need it
2	**clock summer-time recurring** *{<1-4>| last} { sun	mon	tue	wed	thu	fri	sat } {<1-12>	MONTH } <0-23> <0-59> {<1-4>	last} { sun	mon	tue	wed	thu	fri	sat } {<1-12>	MONTH } <0-23> <0-59> <1-1440>*	Configure system time in turn: hour, minute, second, year, month, day *<1-4>:* the starting week, **last** stands for the last week *Sun:* Sunday *Mon:* Monday *Tue:* Tuesday *Wed:* Wednesday *Thu:* Thursday *Fri:* Friday *Sat:* Saturday *<1-12>	MONTH:* month, MONTH stands for the month that you inputs *<0-23>:* hour *<0-59>:* minute *<1-4>	last:* ending week *Last:* the last week *Sun:* Sunday *Mon:* Monday *Tue:* Tuesday *Wed:* Wednesday *Thu:* Thursday *Fri:* Friday *Sat:* Saturday *<1-12>	MONTH:* month, MONTH stands for the month that you inputs *<0-23>:* hour *<0-59>:* minute *<1-4>| last:* ending week
3	**show clock summer-time recurring**	Show summer time configuration

Notice: When configuring the system time manually, if the system uses summer time, then each year April second Sunday morning 2 O' clock to 3 O' clock is not existed. For example, the summer time is set to from

the second Sunday 2:00 am of April to the second Sunday 2:00 am of September each year; when the clock in this time domain is changed one hour faster, or 60 minutes' excursion, then the time between the second Sunday morning 2 and 3am is not existed. The result of manual configuration to the time in this time segment will be failure.

21.2.5 Monitoring and maintenance

Use the following commands to show clock information:

Command	Description
show clock	Show clock information

Use the following commands to show clock information and summer time state:

Command	Description
show clock summer-time-recurring	Show clock summer time

21.2.6 Typical configuration example

Configure the switch time zone and summer time:

Raisecom#**clock timezone** *– 10 30*

    set successfully!

Raisecom#**clock set** *11 14　20　2005　3　28*

    set successfully!

Raisecom#**show clock summer-time-recurring**

    Current system time:　Mar-28-2005　11:15:22

    Timezone offset: -10:30:00

    Summer time recurring: Disable

Raisecom#**clock summer-time enable**

    set successfully!

Raisecom#**clock summer-time recurring** *2* **sun** *3 2 0 2* **sun** *9 2 0 60*

    set successfully!

Raisecom#**show clock summer-time-recurring**

    Current system time:　Mar-28-2005　12:15:53

    Timezone offset: -10:30:00

    Summer time recurring: Enable

    Summer time start: week 02 Sunday Mar　02:00

    Summer time end: week 02 Sunday Sep　02:00

    Summer time Offset: 60 min

21.3 Configure SNTP function

21.3.1 Default SNTP protocol configuration

Function	Default value
SNMP server address	Not existed

21.3.2 Configure SNTP protocol function

When SNTP server address is configured, the equipment will try to get clock information from SNTP server every 10 seconds, and the maximum exceeding time of SNTP getting clock information is 10 seconds.

Step	Command	Description
1	config	Enter global configuration mode
2	**sntp server** A.B.C.D	Configure SNTP server address
3	**exit**	Return to privileged EXEC mode
4	**show sntp**	Show the configuration

21.3.3 Monitoring and maintenance

Use the following commands to show the switch time management running state and configuration.

Command	Description
show clock	Show clock information

21.3.4 Typical configuration example

For example: the topology structure is shown below:
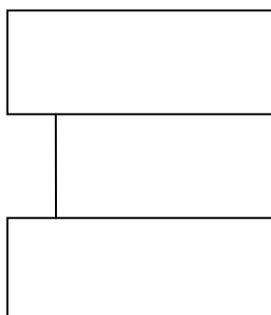
➢ Destination:

The switch will get system time from SNTP server

➢ The configuration steps:

Step 1: show the current default system clock

Raisecom(config)#**show clock**

Current system time: Jan-01-2000   08:00:37

Timezone offset: +08:00:00

Step 2: configure SNTP server address

Raisecom(config)#**sntp server** *10.168.0.184*

set successfully!

JUN-15-2008 20:23:55   CONFIG-6-Get SNTP time , Date   is Jun-15-2008   Time is 20:23:55

Raisecom(config)#**exit**

Step 3: show SNTP configuration

Raisecom#**show sntp**

SNTP server address:10.168.0.184

SNTP Server	*Stratum*	*Version*	*Synchronize Time*
10.168.0.184	*15*	*1*	*2008-6-15 20:23:55*

Step 4: show current system clock

Raisecom#**show clock**

Current system time: Jun-15-2008   20:24:33

Timezone offset: +08:00:00

Chapter 22   ACL

22.1 Configuration Description

This chapter is suit to configuration ACL function on the following devices: ISCOM2812f/2826/ 2826e/2828f/2852, ISCOM2926/2924gf, ISCOM3012f/3026/3026e/3028f/3052, ISCOM2250.

22.2 ACL Introduction

In order to filter packets, network equipment needs to set a series of matching rules to identify the filtered objects. Only after this, user can allow or prohibit relative packets to pass through according to the designated strategy in advance. ACL (Access Control list) is used to realize these operations.

ACL can be applied to VLAN, Layer-2 physical port and Layer-3 management interface.

ACL makes classification to packets according to a series of matching conditions; these conditions can be packet source address, destination address and port number etc. It is combined with a series of judgment sentences. After activating a ACL, switch will check each received packet according to the judgment conditions, packets will be forwarded or dropped then according to these conditions.

User can specify *permit* or *deny* while configuring ACLs. When it is set as *deny*, packets that are in accord with the rules will be dropped, the others will be forwarded; when it is set as *permit*, packets that are in accord with the rules will be forwarded, the others will be dropped.

22.3 IP ACL Configuration

Switch supports 400 IP access control lists at most with corresponding series number 0～399. it specifies classification rules according to the source IP address, destination IP address in the IP packet header, used TCP or UDP protocol port number and etc. packet attributes information, and then processes related operations to the packets according these rules. The construction of IP packet header can be referred to RFC791 and other related documents.

22.3.1 IP ACL Default Configuration

None.

22.3.2 IP ACL Configuration

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**ip-access-list** *list-number {deny |*	*ip-access-list:* configuration IP address access

	permit} protocol {source-address mask | **any**} [*source-protocol-port*] {*destination-address mask |* **any**} [*destination-protocol-port*]	control list *list-number:* IP address access control listserial number, range from 0-399 *deny	permit*: reject/accept access. *protocol* binding protocol type. *source-address mask |* **any**: source IP address with its mask, format is dotted decimal in the form of A.B.C.D, **any** indicates arbitrary address. *source-protocol-port*: source port for TCP/UDP protocol *destination -address mask |* **any:** is the destination address and its mask, the format is dotted decimal as A.B.C.D; **any** indicates arbitrary address. *destination -protocol-port*: the destination port of TCP/UPD.
3	**exit**	Exit global configuration mode and enter privileged EXEC mode
4	**show ip-access-list** *list-number*	Show IP access control list relevant information *list-number* is the series number for the IP access control list to be shown, rang is 0-399.
5	**No ip-access-list** *list-number*	Delete IP access control list *list-number:* the list series number to be deleted

22.3.3 Monitering and Maintenance

Check and display indicated IP ACL command:

Command	Description
show ip-access-list *[{0-399}]*	Show IP Access Control List

22.3.4 Specific Configuration Example:

➢ Destination

Configure source IP address as 192.168.1.0 segment，destination IP address as random address ，protocol type as IP and access type as deny IP access rule;

Configure source IP address is 10.168.1.19; mask is 255.255.255.255; source protocol port is 80; destination address is random port; protocol type is TCP; visit type is deny IP access rule.

Configure source IP address is 10.168.1.19; mask is 255.255.255.255; destination address is 10.168.0.0 segment; protocol type is TCP; access type is permit's IP acess rule.

➢ Set up Steps

Raisecom#**config**

Raisecom(config)#**ip-access-list** *0* **deny ip** *192.168.1.0 255.255.255.0* **any**

Raisecom(config)#**ip-access-list** *1* **deny tcp** *10.168.1.19 255.255.255.255 80* **any**

Raisecom(config)#**ip-access-list** *2* **permit tcp** *10.168.1.19 255.255.255.255 80 10.168.0.0 255.255.0.0 80*

Raisecom(config)#**exit**

Raisecom#**show ip-access-list**

Src Ip: Source Ip Address

Dest Ip: Destination Ip Address

List	*Access*	*Protocol*	*Ref.*	*Src Ip:Port*	*Dest Ip:Port*
0	*deny*	*IP*	*0*	*192.168.1.0:0*	*0.0.0.0:0*
1	*deny*	*TCP*	*0*	*10.168.1.19:80*	*0.0.0.0:0*
2	*permit*	*TCP*	*0*	*10.168.1.19:80*	*10.168.0.0:80*

22.4 MAC ACL Function

Switch supports 400 digital-identified Layer-2 (MAC) access control lists at most with corresponding series number 0～399. Layer-2 access control list in conjunction with filter can process relevant operations to packets according to the source MAC address carried in Layer-2 frame, destination MAC address, source VLAN ID, Layer-2 protocol types and other Layer-2 information rules.

22.4.1 MAC ACL Default Configuration

None.

22.4.2 MAC ACL Configuration

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**mac-access-list** *list-number* {**deny**| **permit**} [*protocol* / **any**] {*source-MAC-address* | **any**} {*destination-MAC-address* / **any**}	MAC access control list configuration *list-number:* access control list series number, range 0-399. *deny*|*permit:* indicates deny/permit access [protocol | **any**]: indicates bonded protocol type, **any** indicates unrestricted protocol type. *source-MAC-address:* indicates the source MAC address to be configured, format is hexadecimal string as "HHHH.HHHH.HHHH", dotted every 4 characters; any indicates arbitrary source MAC address. *destination-MAC-address*: the destination MAC address to be configured, format is hexadecimal string as "HHHH.HHHH.HHHH", dotted every 4 characters; any indicates arbitrary destination MAC address.
3	**exit**	Exit global configuration mode and enter privileged EXEC mode

		Show MAC access control list
4	**show mac-access-list** *list-number*	*list-number:* is the series number for the MAC access control list to be shown, rang is 0-399.
5	**no mac-access-list** *list-number*	Delete configured MAC access control list *list-number:* the list series number to be deleted

22.4.3 Monitoring and Maintenance

Check and display indicated MAC ACL command:

Command	Description
show mac-access-list *[{0-399}]*	Display MAC access control list

22.4.4 Specific Configuration Examples

➢ Destination

Configure source MAC address as 1234.1234.1234; destination MAC address as 5678.5678.5678; protocol as IP; access type as deny's MAC access rule;

Configuration source MAC address as 1111.2222.3333; destination MAC address as 4444.5555.6666; protocol as ARP; access type as permit's MAC access rule.

➢ Set up Steps

Raisecom#**config**

Raisecom#**config**

Raisecom(config)# **mac-access-list** *0* **deny ip** *1234.1234.1234 5678.5678.5678*

Raisecom(config)# **mac-access-list** *1* **permit arp** *1111.2222.3333 4444.5555.6666*

Raisecom(config)#**exit**

Raisecom#**show mac-access-list**

Src Mac: Source MAC Address

Dest Mac: Destination MAC Address

List	*Access*	*Protocol*	*Ref.*	*Src Mac*	*Dest Mac*
0	*deny*	*ip*	*0*	*1234.1234.1234*	*5678.5678.5678*
1	*permit*	*arp*	*0*	*1111.2222.3333*	*4444.5555.6666*

22.5 MAP ACL Function

Switch supports 400 digital-identified access list maps at most with corresponding series number 0～399. Access list map can define more protocols and more detailed protocol character fields than IP access list and MAC access list, also can implement matching to any bytes in the first 64 bytes of Layer-2 frame according to user's definition before corresponding processing to the data packets from matched results. User needs to be familiar with Layer-2 data frame before using user-defined access list map.

Access list map uses command *match* to set the expected matching character field, no conflicts can exist in the same access list map when setting matching character field. Character fields that can be matched are shown below:

- Mac destination address
- Mac source address
- Ethernet protocol type
- CoS
- ARP protocol type
- Hardware address of ARP protocol sender
- Hardware address of ARP protocol receiver
- IP address of ARP protocol sender
- IP address of ARP protocol receiver
- IP protocol destination address
- IP protocol source address
- IP protocol priority
- IP protocol ToS
- IP protocol dscp
- IP protocol segmentation bit
- IP protocol type
- TCP protocol destination port
- TCP protocol source port
- TCP protocol bit
- UDP protocol destination port
- UDP protocol source port
- ICMP protocol information type
- ICMP protocol information code
- IGMP protocol information type

User can also use regular mask and offset to define any byte in the first 64 bytes in data frame, and then compare them with the user-defined rules to obtain the matched data frame, after this user can implement relevant operations. User-defined rules can be certain data fixed attributes, such as that in order to obtain all the TCP packets, user can define the rules as "06", mask as "FF", offset as "27", by using such a method, regular rules and offsets can work together to pick up the segment of TCP protocol number in data frame, then compare it with defined rules to obtain all matched TCP packets.

Attention: Rules should be even hexadecimal, offset includes segment of 802.1Q VLAN TAG even if what the switch receives is untagged packet.

22.5.1 MAP ACL Default Configuration

None.

22.5.2 MAP ACL Congfiguration

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**access-list-map** *list-number* {**deny** | **permit**}	*list-number*: list serial number, from 0-399 *deny* | *permit* deny or permit data packets to go through when matching.
3	**match mac {destination | source}** *HHHH.HHHH.HHHH*	*destination* | *source* match source mac or destination mac

		HHHH.HHHH.HHHH mac address
4	**match cos <0-7>**	<0-7> match cos value
5	**match ethertype** *HHHH [HHHH]*	*HHHH[HHHH]* match Ethernet type [mask]
6	**match** *{arp | eapol | flowcontrol | ip | ipv6 | loopback | mpls | mpls-mcast | pppoe | pppoedisc | x25 | x75}*	*arp:* match ARP protocol *eapol:* match eapol protocol *flowcontrol:* match flow control protocol *ip:* match ip protocol *ipv6:* match ipv6 protocol *loopback:* match loopback protocol *mpls:* matchmpls single cast protocol *mpls-mcast:* matchmpls group cast protocol *pppoe:* match pppoe protocol *pppoedisc:* match pppoe discover protocol *x25:* match x25 protocol *x75:* match x75 protocol
7	**no match mac** *{destination|source}*	Do not match MAC address *destination | source:* match source mac or destination mac
8	**no match cos**	Do not match CoS value
9	**no match ethertype**	Do not match Ethernet type
10	**match arp opcode** *{request |reply}*	Match arp protocol type *request | reply* arpprotocol reply /request packet
11	**match arp** *{sender-mac | target-mac}* *HHHH.HHHH.HHHH*	Match arp protocol hardware address *sender-mac| target-mac:* match arp sender/target mac address *HHHH.HHHH.HHHH:* MAC address
12	**match arp** *{sender-ip | target-ip}* *A.B.C.D [A.B.C.D]*	Match arp protocol IP address *sender-ip | target-ip* sender/target: IPaddress *A.B.C.D [A.B.C.D]:* Ip address [mask]
13	**no match arp opcode**	do not matcharpprotocoltype
14	**no match arp** *{sender-mac | target-mac}*	do not match arp protocol hardware address
15	**no match arp** *{sender-ip | target-ip}*	do not matcharpprotocolIPaddress *sender-ip| target-ip* sender/target IP address
16	**match ip** *{destination-address | source-address} A.B.C.D [A.B.C.D]*	Match IP protocol address *destination-address | source-address* Ip protocol destination/source address *A.B.C.D [A.B.C.D]* IP address [mask]
17	**match ip precedence** *{<0-7>| routine| priority|immediate| flash| flash-override|critical| internet| network}*	Match IP priority *<0-7>:* IP priority value *routine:* IP priority value 0

		priority: IP priority value 1
		immediate: IP priority value 2
		flash: IP priority value 3
		flash-override: IP priority value 4
		critical: IP priority value 5
		internet: IP priority value 6
		network: IP priority value 7
18	**match ip ToS** *{<0-15> | normal | min-monetary-cost | min-delay | max-reliability | max-throughput}*	Match IP priority ToS value *<0-15>:* ToS value *normal:* normal ToS value (0) *min-monetary-cost:* Min monetary cost ToS value(1) *min-delay:* Min delay ToS value(8) *max-reliability:* Max reliability ToS value(2) *max-throughput:* Max throughput ToS value(4)
19	**match ip dscp** *{<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41| af42 |af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | default}*	Match IP DSCP value *<0-63>:* IP DSCP value *af11:* AF11 DSCP value(001010) *af12:* AF12 DSCP value(001100) *af13:* AF13 DSCP value(001110) *af21:* AF21 DSCP value(010010) *af22:* AF22 DSCP value(010100) *af23:* AF23 DSCP value(010110) *af31:* AF31 DSCP value(011010) *af32:* AF32 DSCP value(011100) *af33:* AF33 DSCP value(011110) *af41:* AF41 DSCP value(100010) *af42:* AF42 DSCP value(100100) *af43:* AF43 DSCP value(100110) *cs1:* CS1(priority 1) DSCP value(001000) *cs2:* CS2(priority 2) DSCP value(010000) *cs3:* CS3(priority 3) DSCP value(011000) *cs4:* CS4(priority 4) DSCP value(100000) *cs5:* CS5(priority 5) DSCP value(101000) *cs6:* CS6(priority 6) DSCP value(110000) *cs7:* CS7(priority 7) DSCP value(111000) default*:* Default DSCP value(000000) *ef:* EF DSCP value(101110)
20	**match ip no-fragments**	Match no-fragment IP packet
21	**match ip protocol** *<0-255>*	Match IP protocol value *<0-255>:* IP protocol type value

22	**match ip** *{ ahp |esp|gre|icmp|igmp|igrp |ipinip|ospf|pcp|pim|tcp|udp}*	Match IP protocol value *ahp:* autherize header protocol *esp:* encapsulation security payload protocol *gre:* General routing encapsulation protocol *icmp:* Internet control message protocol *igmp:* Internet group message protocol *igrp:* Interior gateway routing protocol *ipinip:* IP-in-IP tunnel *ospf:* Open shortest path first *pcp:* Payload compression protocol *pim:* protocol independent multicast protocol *tcp:* Transmission control protocol *udp:* user datagram protocol
23	**no match ip** *{destination-address | source-address}*	Do not match IP protocol address *destination-address | source-address:* IP protocol destination/source address
24	**no match ip precedence**	do not match IP priority
25	**no match ip ToS**	do not match IP ToS value
26	**no match ip dscp**	do not match IP DSCP value
27	**no match ip no-fragments**	do not match IP no-fragment
28	**no match ip protocol**	do not match IP protocol value
29	**match ip tcp** *{ destination-port | source-port} {<0-65535> | bgp | domain | echo | exec | finger | ftp | ftp-data | gopher | hostname | ident | irc | klogin | kshell | login | lpd | nntp | pim-auto-rp | pop2 | pop3 | smtp | sunrpc | syslog | tacacs | talk | telnet | time | uucp | whois | www}*	Match Tcp protocol port number *destination-port | source-port:* TCP protocol destination/source port *<0-65535>:* tcp port number *bgp:* border gateway protocol（179） *domain:* domain name service protocol（53） *echo:* echo protocol（7） *exec:* Exec (rsh, 512) *finger:* Finger (79) *ftp:* File transfer protocol（21） *ftp-data:* FTP data connections （20） *gopher:* Gopher (70) *hostname:* NIC hostname server (101) *ident:* identify protocol (113) *irc:* Internet Relay Chat protocol (194) *klogin:* Kerberos login (543) *kshell:* Kerberos shell (544) *login:* Login (rlogin, 513) *lpd:* Printer Service protocol(515)

		nntp: network news transport protocol
		pim-auto-rp: PIM Auto-RP (496)
		pop2: post office protocol v2 (109)
		pop3: post office protocol v3 (110)
		smtp: simple mail transport protocol (25)
		sunrpc: Sun Remote Procedure Call (111)
		syslog: System log (514)
		tacacs: TAC access control system (49)
		talk: Talk (517)
		telnet: Telnet (23)
		time: Time (37)
		uucp: Unix-to-Unix Copy program (540)
		whois: Nicname(43)
		www: World Wide Web (HTTP, 80)
30	**match ip tcp** *{ack | fin | psh | rst | syn | urg }*	Match TCP protocol bit ack: match ACK bit fin: matchFIN bit psh: matchPSH bit rst: matchRST bit syn: matchSYN bit urg: matchURG bit
31	**no match ip tcp** *{ destination-port | source-port}*	do not match Tcp protocol port number destination-port | source-port: TCP protocol destination/source port
32	**no match ip tcp** *{ack | fin | psh | rst | syn | urg }*	do not match TCP protocol bit ack: match ACK bit fin: match FIN bit psh: match PSH bit rst: match RST bit syn: match SYN bit urg: match URG bit
33	**match ip udp** *{ destination-port | source-port } {<0-65535> | biff | bootpc | bootps | domain | echo | mobile-ip | netbios-dgm | netbios-ns | netbios-ss | ntp | pim-auto-rp | rip | snmp | snmptrap | sunrpc | syslog | tacacs | talk | tftp | time | who }*	Match udp protocol port number destination-port | source-port: TCP protocol destination/source port <0-65535>: udp port number biff: Biff (mail notification, comsat, 512) bootpc: bootstrap protocol (BOOTP) client （68） bootps: bootstrap protocol(BOOTP) server（67） domain: domain name service protocol（53） echo: echo protocol（7）

		mobile-ip: mobile IP registration (434)
		netbios-dgm: NetBios datagram eservic（138）
		netbios-ns: NetBios name service（137）
		netbios-ss: NetBios session service（139）
		ntp: network time protocol(123)
		pim-auto-rp: PIM Auto-RP (496)
		rip: routing information protocol(520)
		snmp: simple network magagement protocol(161)
		snmptrap: SNMP Traps (162)
		sunrpc: Sun remote procedure call (111)
		syslog: system log (514)
		tacacs: TAC access control system (49)
		talk: talk (517)
		tftp: trivial file transfer protocol(69)
		time: Time (37)
		who: Who service (rwho, 513)
34	**no match ip udp {** *destination-port* / *source-port}*	do not match udp protocol port number *destination-port* / *source-port:* TCP protocol destination/sourceport
35	**match ip icmp** *<0-255> [<0-255>]*	Match icmp protocol information type *<0-255> [<0-255>]*: information type[information code]
36	**match ip igmp {** *<0-255>	dvmrp / query	leave-v2	report-v1	report-v2 |report-v3	pim-v1 }*	Match igmp protocol information type *<0-255>:* IGMP information type *dvmrp:* Distance Vector Multicast Routing Protocol *leave-v2:* IGMPv2 leave group *pim-v1:* protocol Independent Multicast version 1 *query:* IGMP member query *report-v1:* IGMPv1 member report *report-v2:* IGMPv2 member report *report-v3:* IGMPv3 member report
37	**match user-define** *rule-string rule-mask <0-64>*	Match user-defined segment *rule-string*: user-defined regular string, must be combined of hexadecimal, no more than 64 bytes. *rule-mask*：mask rule, used to implement "or" operation with data packet *<0-64>*: offset，based on dataframe header, and implement "or" operation from the beginning of specified bytes
38	**no match user-define**	do not match user-defined segment
39	**exit**	Exit global configuration mode and enter privileged EXEC mode

	Command	Description
40	**show access-list-map** [*list-number*]	Show port *access-list-map* *list-number* is the port access-list-map series number to show, range is 0-399
41	**no access-list-map** *list-number*	Delete user-defined access-list-map list-number is the list number to delete

22.5.3 Monitoring and Maintenance

Check and display indicated access control list command:

Command	Description
show access-list-map *[{0-399}]*	Display access control list map list

22.5.4 Specific Configuration Example

➢ Destination

To filter bytes 123456 from the 40th bytes in the data frame, access type is "deny". ARP protocol request packet is filtered.

➢ Set up Steps

Raisecom#**config**

Raisecom(config)#**access-list-map** *0* **deny**

Raisecom(config-aclmap)#**match user-define** *123456 ffffff 40*

Raisecom(config-aclmap)#**exit**

Raisecom(config)#**access-list-map** *1 permit*

Raisecom(config-aclmap)# **match arp opcode request**

Raisecom(config-aclmap)#**exit**

Raisecom(config)#**exit**

Raisecom#**show access-list-map**

access-list-map 0 deny

     Match user-define 123456 ffffff 40

access-list-map 1 permit

     Match arp Opcode request

22.6 Application Configuration Based on Hardware ACL

3 steps for using ACL on Layer-2 physical port or VLAN are as follows:：

1. Define ACL

Described in section 1.4.

2. Configuration Filter

After setting up ACL, you need to set the filter. Whether the filter is configured successfully depends on if the global status is enabled or not. You can use specific commands to make ACLs effective or to delete the filters that are already take effects. You can user command **no filter** to disable the related rules, if rules have been written in hardware, they will be deleted from the hardware and configurations.

In a physical port or VLAN filter rule can be composed by multi "permit/deny" statements and every statement indicated different size range of data packet. There is a problem of match order while a data packet and access control rule are matching. The match order of access control rule depends on configuration filter rule's order. The later the order, the higher the priority. If there is conflicts in the rules, high priority will be followed.

There are four kinds of configurations: one is based on switch, one is based on port, on is based from ingress port to egress port, one is based on VLAN. For the filtering rules based on port, you have two options, one of which is based on flow ingress with the other one based on flow egress.

3. Simulate Filter

Use filter command to make the access control rule effect or no effect. Default status is no effect. Once command is configured as effect, not only the earlier configuration filter rules will be effect, but also the later configuration filter rule will effect as well.

22.6.1 Application Default Configuration Based on Hardware ACL

None.

22.6.2 Application Configuration Based on Hardware ACL

➢ Application based on switch

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**[no] filter** *(ip-access-list / mac-access-list / access-list-map) {acllist / all}*	Set filter based on switch **ip-access-list** indicates that the filter uses IP access list **mac-access-list** indicates that the filter uses MAC access list **access-list-map** indicates that the filter uses user-defined access list map *acllist* / **all** access control list series number, all means all the configured access control lists
3	**filter** *(enable / disable)*	**enable** filter function effect enable **disable** filter function effect disable
4	**exit**	Exit global configuration mode and enter privileged EXEC mode
5	**show filter**	Show all filter status

➢ Application based on port

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**[no] filter** (**ip-access-list | mac-access-list | access-list-map**) {*acllist* / **all**} {**ingress / egress** } **port-list** {*portlist* }	Set filter based on port **ip-access-list** indicates that the filter uses IP access list **mac-access-list** indicates that the filter uses MAC access list **access-list-map** indicates that the filter uses user-defined access list map **acllist | all** access control list series number, **all** means all the configured access control lists **ingress | egress** means to carry out the filtering on ingress|egress **port-list** the filter is applied to port portlist Phsical port list range
3	**filter** *(enable | disable)*	**enable** filter function effect enable **disable** filter function effect disable
4	**exit**	Exit global configuration mode and enter privileged EXEC mode
5	**show filter**	Show all filter status

➢ Based from ingress port to egress port

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**[no] filter (ip-access-list | mac-access-list | access-list-map)** {**all**/ *acllist*} **from** *ingress-port* **to** *egress-port*	Set the filter based from ingress port to egress port **ip-access-list** indicates that the filter uses IP access list **mac-access-list** indicates that the filter uses MAC access list **access-list-map** indicates that the filter uses user-defined access list map acllist | **all** access control list series number, **all** means all the configured access control lists from to directions **ingress-port** ingress port **egress-port** egress port
3	**filter** *(enable/disable)*	*enable:* filter function effect enable *disable:* filter function effect disable
4	**exit**	Exit global configuration mode and enter privileged EXEC mode
5	**show filter**	Show all filter status

➤ Application based on VLAN

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**[no] filter (ip-access-list | mac-access-list | access-list-map) {all/** *acllist*} **vlan** *vlanid*	Set the filter based on VLAN **ip-access-list** indicates that the filter uses IP access list **mac-access-list** indicates that the filter uses MAC access list **access-list-map** indicates that the filter uses user-defined access list map **acllist | all** access control list series number, **all** means all the configured access control lists **Vlan** the filter is applied to VLAN **vlanid** VLAN ID
3	**filter (enable | disable)**	**enable** filter fuction effect enable **disable** filter fuction effect disable
4	**exit**	Exit global configuration mode and enter privileged EXEC mode
5	**show filter**	Show all filter status

22.6.3 Monitoring and Maintenance

Check and display all configuration filter status command:

Command	Description
show filter	Display all configuration filter status

22.6.4 Specific Configuration Examples

Example 1:

➤ Destination

The switch does not allow TCP packet to pass through with destination port 80

➤ Set up steps

Raisecom#**config**

Raisecom(config)# **ip-access-list** *0* **deny tcp any any** *80*

Raisecom(config)# **filter ip-access-list** *0*

Raisecom(config)#**filter** *enable*

Raisecom(config)#**exit**

Example 2:

> Destination

The switch does not allow ARP packets with the MAC address 000e.3842.34ea to pass through on port 2 to 8.

> Set up Steps

Raisecom#**config**

Raisecom(config)# **mac-access-list** *2* **deny arp any** *000e.3842.34ea*

Raisecom(config)# **filter mac-access-list** *2* **ingress portlist** *2-8*

Raisecom(config)#**filter** *enable*

Raisecom(config)#**exit**

Example 3:

> Destination

The switch allows IP packets with the source address in network segment 10.0.0.0/8 to pass through in VLAN 3

> Set up Steps

Raisecom#**config**

Raisecom(config)# **ip-access-list** *2* **deny ip any any**

Raisecom(config)# **ip-access-list** *3* **permit ip** *10.0.0.0 255.0.0.0* **any**

Raisecom(config)# **filter ip-access-list** *2,3* **vlan** 3

Raisecom(config)#**filter** *enable*

Raisecom(config)#**exit**

22.7 Configuration Function Based on Software IP ACL

The steps below show how to use software IP ACL on Layer-3 interface:

1） Define access control list

Show in section 1.2

2） ACL Configuration

Filtering rules on a Layer-3 interface can be combined of one or multiple "permit | deny" sentences, every sentence has different specified packet ranges, so matching order problem may happen when matching one packet and ACL rule. The matching order depends on the orders of configured filtering rules, as the order closer to the back, the higher the priority will be. When conflict happens, high priority will be the benchmark.

22.7.1 Application Default Configuration Based on Software IP ACL

None

22.7.2 Layer-3 Interface Protect Configuration Based on IP ACL

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**interface ip** *<0-14>*	Enter Layer-3 interface configuration mode
3	**[no] ip ip-access-list** {**all**/ *acllist*}	Set Layer-3 interface filter **ip-access-list** indicates that the filter uses IP access list acllist | **all** access control list series number, **all** means all the configured access control lists
4	**exit**	Exit Ethernet Layer-3 interface configuration mode and enter global configuration mode
5	**exit**	Exit global configuration mode and enter privileged EXEC mode
6	**show interface ip ip-access-list**	Show filters status for all interfaces

22.7.3 Monitoring and Maintenance

Check and display configuration filter status command:

Command	Description
show interface ip ip-access-list	Show all filters status for Layer-3 interface

22.7.4 Specific Configuration Example

Example 1:

➢ Destination

Switch only allow IP packet with 10.0.0.0/8 access

➢ Set up steps

Raisecom#**config**

Raisecom(config)# **ip-access-list** *2* **deny ip any any**

Raisecom(config)# **ip-access-list** *3* **permit ip** *10.0.0.0 255.0.0.0* **any**

Raisecom(config)#**interface ip** *0*

Raisecom(config-ip)# **ip ip-access-list** *2,3*

Raisecom(config-ip)#**exit**

Raisecom(config)#**exit**

Chapter 24   QoS

23.1 Configuration Description

This configuration paper is suit to the following situations:

For transceiver device: to guide the user to configuration QoS function except for Policy and class function;

For Switch device: to guide the user to configuration most Qos function on the most Switch device , except for some exception. User can look up the QoS function command one to the QoS function command nine to see the details.

23.2 QoS Introduction

24.2.1 Introduction

Generally speaking, Internet (Ipv4 standard) provides users only "best effort" service, cannot guarantee a real-time and complete packets transmission, and the quality of services either. Since user always has different requirements for the transmission quality of separate multi-media applications, network resources should be redistributed and scheduled according to user's demands. By using network quality of service, user is able to process specific data traffic with higher priority, or applies particular management schedule strategy to make the network more predictable and the bandwidth management more effective.

1. QoS Basis

ISCOM2800 mechanism realizes layer-2 packets classification based on 802.1P and 802.1Q standards. 802.1Q defines VLAN, though QoS is not defined in this standard, the given mechanism which mention than the frame precedence can be modified configures a strong groundwork to realize QoS. 802.1P standard defines priority mechanism. If packets with high priority have not been transmitted, packets with low priority will not be transmitted.

In Layer-2 802.1Q frame header, there are 2 bytes of TAG control information string, the first 3 bits carry CoS (Class of Service) value, the values is from 0 to 7, shown in the figure below:

Encapsulated Packet

Layer 2 header	IP header	Data

Layer 2 ISL Frame

ISL header (26 bytes)	Encapsulated frame 1... (24.5 KB)	FCS (4 bytes)
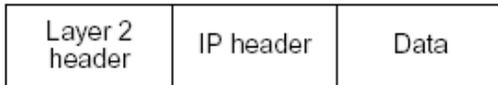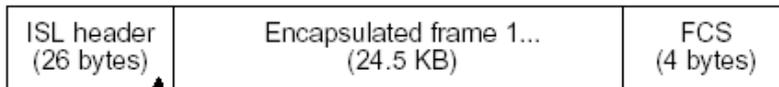
└─ 3 bits used for CoS

Layer 2 802.1Q/P Frame

Preamble	Start frame delimiter	DA	SA	Tag	PT	Data	FCS
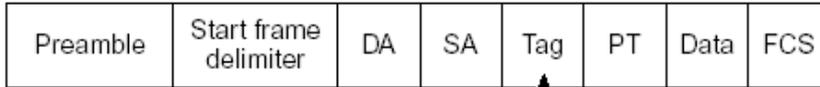
└─ 3 bits used for CoS (user priority)

Layer 3 IPv4 Packet

Version length	ToS (1 byte)	Len	ID	Offset	TTL	Proto	FCS	IP-SA	IP-DA	Data

└─ IP precedence or DSCP

The 8 priority defined by CoS can be considered as the following 8 kinds of packets: Priority	Message type	Application
000	Routine	Level 0 corresponds to the default of the best efforts of the information delivery
001	Priority	Level 1 ~ 4 are corresponds for the definition of multi-media data or important enterprise data.
010	Intermediate	
011	Flash	
100	Flash Override	
101	Critical	Level 5 or 6 is used in the sensitive-delay inter-act video/audio data
110	Internet Control	
111	Network Control	Level 7 is applied for the important high-level network data stream, such as routing information

2. QoS basic mode

✧ Actions at ingress ports include traffic classification, policing and marking:

➢ Classifying: to classify the traffic. This process generates a inner DSCP to identify the data's QoS characteristics.
➢ Policing: Comparing inner DSCP and configured policies to determine whether the packet goes into the policy profile or out. Policy limits the occupied bandwidth. The results will be sent to marker.
➢ Marking: Evaluates the policy and configuration information for the action to be taken when a packet is out of profile and determines what to do with the packet (pass through a packet without modification, mark down the QoS label in the packet, or drop the packet).

✧ Actions at the egress port include queueing and scheduling:

➢ Queueing: evaluates the QoS packet label and the corresponding DSCP before selecting which queues to use. The DSCP value is mapped to an inner CoS value for the seletion of an output queue.
➢ Scheduling: based on configured WRR (Weighted round robin) and threshold to provide service for output queue.

Actions at egress

Actions of ingress

✧ The figure below shows the QoS basic model:

```
                                    ┌─────────────────┐
                                    │ Queueing and    │
                                    │ scheduleing     │
                                    │ Actions of      │
                                    │ ingress         │
                                    └─────────────────┘
```

24.2.2 Classification

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet.Classification works only when the global QoS function is enabled. QoS is disabled by default.You specify which fields in the frame or packet that you want to use to classify incoming traffic.
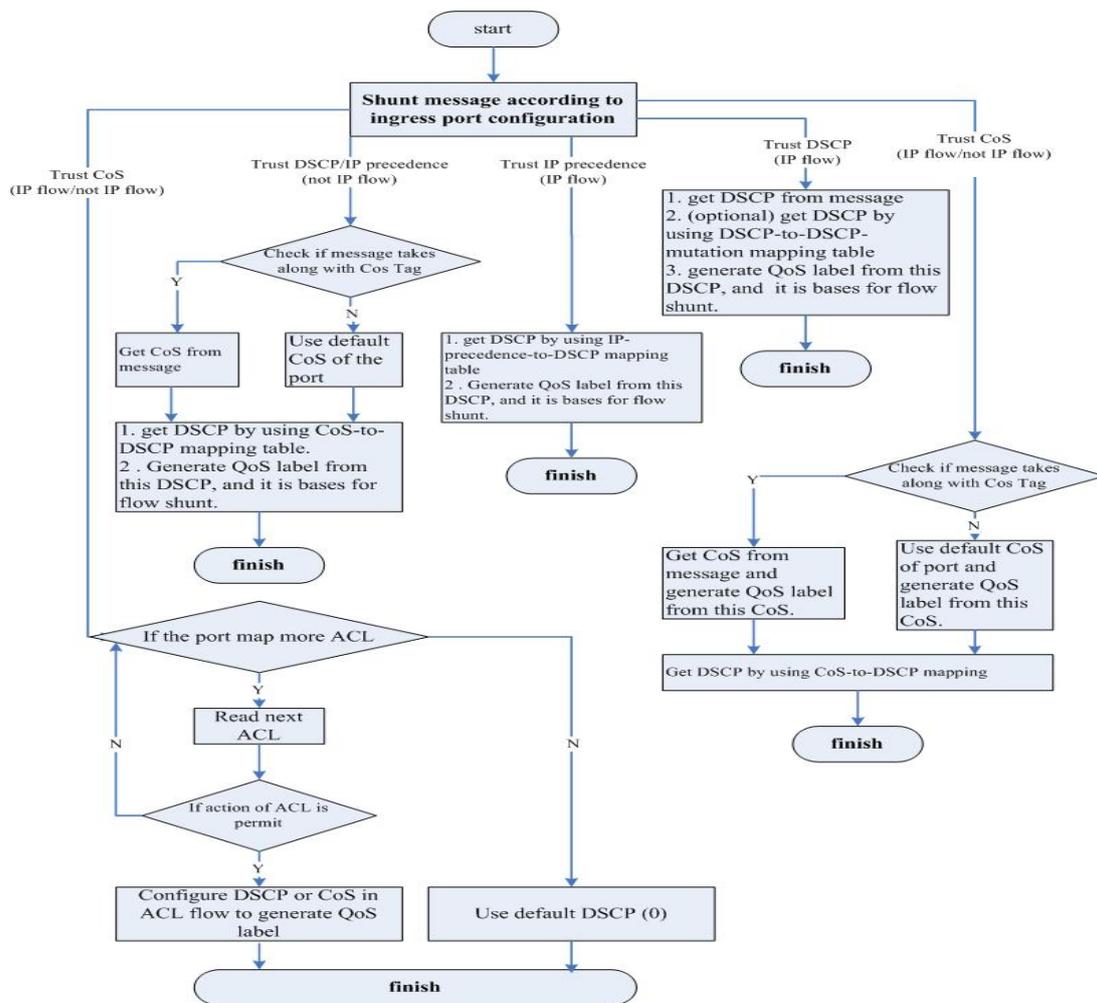
Description:

✧ For none-IP traffic, the classification procedure is as follows:

➢ Use port default value: if the data frame does not have CoS value, assign the incoming frame with the port default Cos value, and then use CoS-to-DSCP map to generate inner DSCP value.

➢ TRUST the CoS value of input frame (configure the port as TRUST COS): use configurable CoS-to-DSCP mapping table to generate inner DSCP value. For none-IP traffic, whether to configure it as DSCP TRUST and IP precedence TRUST is meaningless, system will use port default CoS value.
➢ Based on configured Layer-2 MAC ACL classification, check the source MAC, destination MAC and Ethernet field. If there is no configured ACL, assign the default DSCP value as 0. Otherwise, assign DSCP value to the incoming frame based on policy mapping table.

✧ For IP traffic:

➢ TRUST IP DSCP value of incoming packets (configure the port as TRUST DSCP): use DSCP of IP packets as the inner DSCP value. You can use DSCP-to-DSCP mapping table to modify the DSCP value if the port is edge port of two QoS domains.
➢ TRUST IP precedence of incoming packet (configure the port as TRUST IP precedence): use IP-precedence-to-DSCP mapping table to generate DSCP value.
➢ TRUST CoS value of incoming packets: use CoS-to-DSCP mapping table to generate DSCP value.
➢ Based on configured IP ACL for classification, check every field in IP packet header. If no ACL is configured, assign the default DSCP value as 0 to the packet. Otherwise, to assign DSCP value to the packet according to policy map.

As described in the diagram, not only we can classify the traffic by different traffic configuration port "TRUST", and the message CoS, DSCP, IP-precedence; but also we can classify the traffic more flexible by the ACL function, class-map.

Attention: The use of two classification ways are multually exclusive and later configuration will take effects.

Class-map mechanism describe data flow classification on ACL:

1. Classification based on QoS ACL:

1) If a matched permit ACL (the first one) is found, related QoS actions will be activated.

2) If a matched deny ACL is found, ignore this one, and go on to the next one.

3) If all ACLs are checked but no matched permit ACL, packet will not be processed.

4) When matching multiple ACLs, implement QoS processing as the first permit ACL is found.

5) After defining an ACL claasification, user can bond it to a policy. Policies include class classification (such as aggregation) or rate limiting, bond the policy to a port before taking effects.

2. Classification based on class-map:

A class map is a mechanism that you use to isolate and name a specific traffic flow (or class) from all other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it:

1) by ACL match

2) by DCSP, IP priority match.

24.2.3 Policy and Marking

1. Policy map

Each policy may have a lot of class-maps, to identify those flow movements.

2. Policy action

In each policy, different actions identify different flow movements. So far, there are 6 actions:

✓ TRUST: the TRUST status of flow as TRUST CoS, DSCP and ToS;

✓ Set: modify the data packets of flow into new value include CoS, DSCP, ToS;

✓ Policy: limit the speed of streams and modify them, also notice what actions are going to use if the flow is over speed limit.

✓ Set VLAN: VLAN coverage.

✓ Re-direct to port: redirect message.

✓ Copy-to-mirror:flow image.

3. Policy Application

A policy mapping is needed to binding on the IN/OUT port to be effective.

24.2.4 Bit-Rate Limitation and Reshaping

QoS uses policy for speed limiting and reshaping, also modify the DSCP data packet or byte losing.

1. Three types of policy:

single-policy: each rule of class-map is using this policy individually.

class-policy: all rules of each class-map are sharing this policy.

aggregate-policy: all class-map of one policy-map are sharing this policy.

If the flow bit rate is out profile, each policy will have two actions: either drop or marked down DSCP value.

2. Policy uses token bucket algorithm

When the switch receives a frame, a token will be added on the bucket. According to the indicated average bit rate, each token is added on the bucket after the swtich checked the available space on the bucket. If not, the packet will be marked as nonconforming, then follow the policy actions(drop or modify). Moreover, burst will cause the actions as well.

24.2.5 Mapping Table

During QoS processing, switch describes the inner DSCP precedence for all traffics:

1. During the classification procedure, QoS use configured map table (CoS-to-DSCP 、 IP-precedence-to-DSCP), based on the CoS or IP precedence value in the incoming packet to obtain an inner DSCP value; To configure DSCP TRUST status on port, if the DSCP values are different in the two QoS domains, use can use DSCP-to-DSCP-mutation map to modify DSCP value.

2. During the policing procedure, QoS can assign new DSCP values to IP or non-ip packets (if the packet is out of profile and the policy has indicated mark down action), this map is called policed-DSCP mapping.

3. Before traffics go into the scheduling, QoS use DSCP-to-CoS map to obtain CoS value according to inner DSCP value, and then use CoS-to-egress-queue map to select the egress queuing.

Attention: If the map table of DSCP-to-DSCP-mutation and policed-DSCP is empty，the default will be the DSCP value of incoming packet;

DSCP-to-DSCP-mutation mapping table is applied for the port, other mapping tables are applied for the switch.

24.2.6 Queueing and Scheduling

Queueing and scheduling will be carried out for packets processing after policing and marking. ISCOM switch realizes two kinds of processing according to different classified packets:

1. Regenerate packet COS value according to the defined rules while maintaining the packet's native COS value

2. The policy is effective only when the rules are configured as relying on TOS value, that is to say: modify the packet's native COS value according to TOS value.

ISCOM series switches support 4 kinds of priority output queues, the priority values are 0-3. The highest priority is level 3; the switch also supports 3 kinds of queue scheduling policies: strict priority scheduling, control forward weight scheduling and control forward delay scheduling.

ISCOM serises switches also support the processing of untagged Layer-2 frame. Every port has default priority which is COS value. When the port receives an untagged packet, the switch will consider the port default priority as the packet's COS value for queue dispatching and scheduling. After the packet goes out of the switch, it will   Renew to the original format.

24.2.7 QoS Default Configuration

No.	Attribute	Default configuration
1	QoS enable	Disable
2	Global QoS Trust Status	UNTRUST
3	Port QoS Trust Status	UNTRUST
4	Port Default CoS	0
5	Port Default DSCP	0
6	Port Default CoS override	Disable
7	Port Default DSCP override	Disable
8	class-map match type	match-all
9	Policy Trust Status	DSCP
10	Queue scheduling policy	Strict priority secheduling SP

CoS-DSCP default map:

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

IP-Precedence-DSCP default map:

ToS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

DSCP-CoS default map:

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS	0	1	2	3	4	5	6	7

DSCP-to-DSCP-Mutation default map(default-dscp):

DSCP	0	1	2	3	4	5	6	7
0	8	9	10	11	12	13	14	15
1	16	17	18	19	20	21	22	23
2	24	25	26	27	28	29	30	31
3	32	33	34	35	36	37	38	39
5	40	41	42	43	44	45	46	47
6	48	49	50	51	52	53	54	55
7	56	57	58	59	60	61	62	63

Inner CoS to queue map:

Inner CoS value	0	1	2	3	4	5	6	7
Queue ID	1	1	2	2	3	3	4	4

23.3 QoS Enable and Disable

23.3.1 QoS Start and Stop Default Configuration

No.	Attributes	Default configuration
1	QoS start	Disable

23.3.2 QoS Start and Close Default Configuration

Under the default situation, QoS is disabled. Use the command below to enable QoS function under global configuration mode.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mls qos**	Enable QoS

3	**Exit**	Back to privileged EXEC mode
4	**show mls qos**	Show QoS configuration status

In order to diable QoS, implement command **no mls qos**.

Before enabling QoS, some functions are still effective, such as port default CoS, port default DSCP, queue scheduling mode, CoS to queue map and so on. Users are suggersted to disable the flow control function before enabling QoS.

23.3.3 Monitoring and Maintenance

Command	Description
show mls qos	Show QoS switch status

23.3.4 Configuration Examples

Open QoS function:

Raisecom#**config**

Raisecom(config)#**mls qos**

Raisecom#**show mls qos**

Show as below:

QoS is enabled.

23.4 Classification Function Configuration

23.4.1 Classification Default Configuration

Function	Default Value
Global QoS TRUST status	UNTRUST
Port QoS TRUST status	UNTRUST
Port default CoS	0
Port default DSCP	0
Port default CoS override	Disable
Port default DSCP override	Disable
Class-mapbmatch type	match-all

23.4.2 Flow Classification Configuration Based on Port TRUST Status

Attention:

➢ Port TRUST status and ACL/Class-map flow classifation are mutually exclusive, and later configuration will take effects.

- ➢ Global and port QoS TRUST status configurations are used for different devices. So far, it is not capable for those two configurations in one equipement.
- ➢ QoS TRUST status configuration and TRUST policy status configuration are mutually exclusive, and later cofniguration will take effects

24.4.2.1 Configuring Global QoS TRUST status

Configure QoS TRUST status for all ports.   Reverse command: **no mls qos TRUST.**

Steps	Command	Description
1	**Config**	Entry to global configuration mode
2	**mls qos TRUST [***cos* / *dscp* / *ip-precedence***]**	All QoS TRUST status ports configuration *cos*: configuration the switch as TRUST CoS status *dscp*: configuartion the switch as TRUST DSCP status *ip-precedence*: configuration the switch as TRUST IP priority status.
3	**Exit**	Return to privileges mode
4	**show mls qos port**	Show QoS port configuration

Configuration example:

Raisecom#**config**

Raisecom(config)#**mls qos** *TRUST* **cos** //**configure port** *TRUST* **status**

Raisecom(config)#**exit**

Raisecom# **show mls qos port**

Show results as:

TRUST state: TRUST CoS

Port Id   Default CoS

----

1   0

2   0

        ……

24.4.2.2 Configuring QoS port TRUST status

configure QoS port TRUST status. In default situation, the switch TRUST status is UNTRUST. Reverse Command is: **no mls qos TRUST.**

Steps	Command	Description
1	**config**	Entry to global configuration mode
2	**interface port** *portid*	Entry to port configuration mode
3	**mls qos TRUST [***cos* / *dscp***]**	Set QoS TRUST mode cos: set port as TRUST CoS status

		dscp:set port as TRUST DSCP status
4	**Exit**	Return to global configuration mode
5	**Exit**	Return privileges mode
6	**Show mls qos port** *portid*	Show QoS port configuration

24.4.2.3 Configuring CoS port default

Only if the port TRUST status is CoS, configuring default CoS takes effects. When the message is untag，CoS default port as CoS value. In default situation, that value will be 0。Reverse command：**no mls qos default-cos**。It can be set under port mode.

Steps	Command	Description
1	**config**	Entry to global configuration mode
2	**interface port** *portid*	Entry to port cofiguration mode
3	**mls qos default-cos** *cos-value*	Set default CoS value CoS-value：set default port CoS value 0-7
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileges mode
6	**Show mls qos port** *portid*	Show QoS port configuration

Configuration example: in Port 1, configure TRUST status as CoS，and when the incoming message is as untag，the CoS value will be 2.

Raisecom#**config**

Raisecom(config)#**inter port** *1*

Raisecom(config-port)#**mls qos** *TRUST cos*   //configure port TRUST status

Raisecom(config-port)# **mls qos default-cos** *2*   //configure CoS port default

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom# **show mls qos port** *1*

Show results as:

Raisecom#**sh mls qos port** 1

Port 1:

TRUST state: TRUST CoS

Default CoS: 2

Default DSCP: 0

DSCP override: Disable

DSCP mutation map: default-dscp

24.4.2.4 Configuring default port DSCP

Only if the port TRUST status is DSCP, the default configuration DSCP takes effect. When the incoming message of DSCP is 0, default port DSCP is used as DSCP value. In default situation, that value is 0. reverse command is: no mls qos default-dscp. It can be set up in port mode:

Steps	Command	description
1	**Config**	Entry into global configuration mode
2	**Interface port** *portid*	Entry into port configuration mode
3	**mls qos default-dscp** *dscp-value*	Set default DSCP value dscp-value: est default port DSCP value as 0-63
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privilege mode
6	**show mls qos port** *portid*	Show QoS port configuration mode

The configuration is similar to CoS port default configuration.

24.4.2.5 Configuring port CoS override (Support equipment is not available)

Only if the port TRUST status is CoS, port CoS override configuration takes effect. Whether incoming message is untag or tag, CoS override value is used as CoS value. In Default situation, there will be no override. Reverse command: **no mls qos default-cos override**。 It can be set up in port mode:

Steps	Command	Description
1	**Config**	Entry into global configuration mode
2	**Interface port** *portid*	Entry into port configuration mode
3	**mls qos default-cos override**	Set CoS override value
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privilege mode
6	**show mls qos port** *portid*	Show QoS port configuration

24.4.2.6 Configuring port DSCP override

Only if port TRUST status is DSCP,that configuration takes effect. Whatever the incoming message DSCP is, DSCP override value is used as DSCP value. In default situation, there will be no override. Reverse command: **no mls qos default-dscp override**.It can be set in port mode:

Steps	Command	Description
1	**Config**	Entry into global configuration mode
2	**interface port** *portid*	Entry into port configuration mode
3	**mls qos default-dscp override**	Set default DSCP value
4	**Exit**	Entry into global configuration mode
5	**exit**	Return to privilege mode

6	**show mls qos port** *portid*	Show QoS port configuration

Configuration example: set TRUST status as DSCP in port 1 and port DSCP override value as 2.

Raisecom#**config**

Raisecom(config)#**inter port** *1*

Raisecom(config-port)#**mls qos** *TRUST dscp*   //set port TRUST status

Raisecom(config-port)# **mls qos default-dscp** *2*

Raisecom(config-port)# **mls qos default-dscp** *override*   //set port DSCP override value as 2

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom# **show mls qos port** *1*

Show results:

Raisecom#**sh mls qos port** *1*

   Port 1:

   TRUST state: TRUST DSCP

   Default CoS: 0

   Default DSCP: 2

   DSCP override: Enable

   DSCP mutation map: default-dscp

23.4.3 Configuring Flow Classification on ACL/class-map

24.4.3.1 Create delete class-map

Class-map is used to isolate the specific data stream, matching conditions include ACL, IP priority and DSCP, VLAN and class.

Creating **class-map** follows the steps below:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**Class-map** *class-map-name* [*match-all*/*match-any*]	Create name as aaa, class-map and entry into config-cmap mode. *class-map-name:* class-map name, Max 16 characters match-all: satisfy all rules in class match-any: satisy only one rule in class
3	**description** *WORD*	Description of information *WORD*: description of information in class map, max 255 characters.
4	**exit**	Return to global configuration mode

5	**exit**	Return to privilege mode
6	**show class-map** [WORD]	Show CLASS MAP WORD: class-map name, max 16 characters

Class-map has two matching types: match-all runs AND operation, as multi match statements and operation. If there is conflict, then the match states fail; match-any is run or operation and default is match-all.

Configuration examples:

Raisecom#**config**

Raisecom(config)# **class-map** *aaa* **match-all**

Raisecom(config-cmap)# **description this-is-test-class**

Raisecom(config-cmap)#**exit**

Raisecom(config)#**exit**

Raisecom#**show class-map**

Show results as:

> *Class Map match-all aaa (id 0)*
>
> *Description:this-is-test-class*
>
> *Match none*

If **class-map** is needed to delete, run **no**,   as **no class-map** *class-map-name***.**

Attention:

- ➢ If class-map is quoted by policy in the port, then it is not able to be deleted.
- ➢ When matching configuration of class-map is match-all, the configuration may fail becasue the matching message may have conflicts.
- ➢ When a ACL is matched, ACL must be indetified and its type must be permit.
- ➢ When a class-map is matched, sub class-map must be match-all type.

24.4.3.2 Configuring match statements

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**class-map** *class-map-name*	Entry into config-cmap mode *class-map-name*：class-map name，max 16 characters
3	**match** {*ip-access-list / mac-access-list / access-list-ma*} *acl-index*	Match ACL *ip-access-list*: match IP access list *mac-access-list*: match MAC access list *access-list-map*: match access control list map table *acl-index*: acess control list index
4	**match ip dscp** {*0-63*}	Match DSCP value
5	**match ip precedence** {*0-7*}	Match ToS value
6	**match vlan** {*1-4094*}	Match VLAN

7	**match class-map** *WORD*	Match class map WORD：match class-map name，max16 characters
8	**exit**	Return to global configuration mode
9	**exit**	Return to privilege mode
10	**show class-map** *[WORD]*	Show CLASS MAP WORD： class-map name，max 16 characters

Attention:

➢ When access control list is matched, ACL must be created first.
➢ When class map is matched, class-map must be created first.
➢ If the match type of class-map is match-all, the configuration may fail because there be conflicts in matched messages.
➢ If the same class-map has been applied for some port, then it is not allowed to modify the match statement.

To delete some match statement:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**class-map** *class-map-name*	Entry into config-cmap mode *class-map-name*：class-map name, max 16 characters
3	**no match** {*ip-access-list* / *mac-access-list* / *access-list-map*} *acl-index*	Match ACL *ip-access-list*: match IP access list *mac-access-list*: match MAC access list *access-list-map*: match access control list map ta ble *acl-index*: access control list index
4	**no match ip dscp** {*0-63*}	Match DSCP value
5	**no match ip precedence** {*0-7*}	Match ToS value
6	**no match vlan** {*1-4094*}	Match VLAN
7	**no match class-map** *WORD*	Match class map WORD：Match class-map name，max 16 characters
8	**exit**	Return to global configuration mode
9	**exit**	Return to privilege mode
10	**show class-map** [*WORD*]	Show CLASS MAP message *WORD*: class-map name，max 16 characters

Attention: If the class-map has already been applied for some other port, it is not allowed to delete the match statement.

23.4.4 Monitering and Maintenance

Command	Description
show mls qos port *[portlist]*	Show QoS port information *portlist*: port number list
show class-map *[WORD]*	Show CLASS MAP information *WORD*: class-map name, max 16 characters

Show QoS port information

Attention: Show different information according to the supports of different equipements. There are the examples for supports of all configurations as show below.

Raisecom#**show mls qos port** *1*

> *port 1:*
>
> *Attached policy-map: aaa*
>
> *TRUST state: not TRUSTed*
>
> *default COS: 2*
>
> *default DSCP: 3*
>
> *DSCP override: disable*
>
> *DSCP Mutation Map: aaa*

If all port information is needed to check:

Raisecom#**show mls qos port**

> *port 1:*
>
> *Attached policy-map: aaa*
>
> *TRUST state: not TRUSTed*
>
> *default COS: 2*
>
> *default DSCP: 3*
>
> *DSCP override: disable*
>
> *DSCP Mutation Map: aaa*
>
> *port 2:*
>
> *Attached policy-map: aaa*
>
> *TRUST state: not TRUSTed*
>
> *default COS: 2*
>
> *default DSCP: 3*
>
> *DSCP override: disable*
>
> *DSCP Mutation Map: aaa*
>
> *......*
>
> *port 26:*

TRUST state: not TRUSTed

default COS: 0

default DSCP: 0

DSCP override: disable

DSCP Mutation Map: default-dscp

Show QoS class-map information:

Raisecom#**show class-map**

Class Map match-all aaa (id 0)

Match ip-access-list 1

Match ip dscp 2

Match class-map bbb

Match vlan 1

Class Map match-all bbb (id 1)

Match ip-access-list 2

If it is needed to show the specific name of class-map, use commands as below:

Raisecom#**show class-map** *aaa*

Class Map match-all aaa (id 0)

Match ip-access-list   1

Match ip dscp 2

Match class-map bbb

Match vlan 1

23.4.5 Typical Configuration Examples

Configuration examples: classify the flow and satisfy the flow in aaa condition: in VLAN1, DSCP is 2 and the messages are from 10.0.0.2 and 10.0.0.3.

Raisecom#**config**

Raisecom(config)# **ip-access-list** *1* **permit ip** *10.0.0.2 255.255.255.0* **any**

Raisecom(config)# **ip-access-list** *2* **permit ip any** *10.0.0.3 255.255.255.0*

Raisecom(config)# **class-map** *bbb* **match-all**

Raisecom(config-cmap)#**match ip-access-list** *2*

Raisecom(config)# **class-map** *aaa* **match-all**

Raisecom(config-cmap)#**match ip-access-list** *1*

Raisecom(config-cmap)#**match ip dscp** *2*

Raisecom(config-cmap)#**match vlan** *1*

Raisecom(config-cmap)#**match class-map** *bbb*

Raisecom(config-cmap)# **exit**

Raisecom(config)#**exit**

Raisecom#**show class** *aaa*

Show results as:

Raisecom#**show class** *aaa*

Class Map match-all aaa (id 0)

Match ip-access-list 1

Match ip dscp 2

Match class-map bbb

Match vlan 1

24.5　Policy and Marking Function Configuration

23.5.1 Policy and Marking Default Configuration

Function	Default value
Policy TRUST status	DSCP

23.5.2 Policy and Marking Configuration

23.5.2.1　Create delete policy-map

Use **policy-map** command to encapsulate and classify the data flow of class-map. Create **policy-map** as the steps below:

Steps	Command	Description
1	**Config**	Entry into global configuration mode
2	**policy-map** *policy-map-name*	Create name as bbb, policy-map and entry into config-pmap mode. policy-map-name: policy map name, max 16 characters
3	**description** *WORD*	Description informaiton WORD: policy map description information, max 255 characters
4	**Exit**	Return to global configuraiton mode
5	**Exit**	Return to privilege mode
6	**show policy-map [***WORD***]**	Show POLICY MAP information *WORD*: policy map name，max 16 characters

Configuration examples:

Raisecom#**config**

Raisecom(config)# **policy-map** *bbb*

Raisecom(config)# **exit**

To check wether the configuration is right, use show command:

Raisecom#**show policy-map**

  Policy Map bbb

  Description:this-is-test-policy

If it is needed to delete a **policy-map**, use **command no**, **no policy-map** *policy-map-name***.**

Attention:

If a policy-map is applied for other ports, then it is not able to be deleted.

23.5.2.2   Define policy map

To define one or more defined class-map as a policy, following steps below are used:

Steps	Command	Descriptions
1	**config**	Entry into global configuration mode
2	**policy-map** *policy-map-name*	Entry into config-pmap mode policy-map-name: policy map name, max 16 characters
3	**class-map** *class-map-name*	Encapsulate cuclass-map aaa into policy aaa, and entry into config-pmap-c mode *class-map-name:*class-map name, max 16 characters
4	**exit**	Return to config-pmap mode
5	**exit**	Return to global configuration mode
6	**exit**	Return to privilege mode
7	**show policy-map [WORD]**	Display POLICY MAP information WORD ： policy map name，max 16 characters
8	**show policy-map class {*WORD*}**	Display POLICY MAP some classification information *WORD:* class-map name, max 16 characters

One class can be applied for many policy.

Configuration examples:

Raisecom#**config**

Raisecom(config)# **policy-map aaa**

Raisecom(config-pmap)# **class-map aaa**

Raisecom(config-pmap-c)#**exit**

Raisecom(config-pmap)#**exit**

Raisecom(config)# **exit**

To check wether the configuration is right, use show command:

Raisecom#**show policy-map**

Policy Map aaa

Class aaa

To delete class-map from a policy:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**policy-map** *policy-map-name*	Entry into config-pmap mode policy-map-name：policy map name，max 16 characters
3	**no class-map** *class-map-name*	Delete class-map from policy *class-map-name*：class-map name，max 16 characters
4	**exit**	Return privilege mode
5	**show policy-map** [*WORD*]	Display POLICY　MAP information *WORD*: policy map name，max 16 characters

Attention: It is not allowed to delete class-map if the policy-map has been applied for some other port.

23.5.2.3　Define policy action

Different actions are used for different data flow in policy, show as below:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**policy-map** *policy-name*	Entry into config-pmap mode policy-name: policy map name, max 16 characters
3	**Class-map** *class-name*	Encapsulate class-map into policy, and entry into config-pmap-c mode *class-name:* class-map name, max 16 characters
4	**police** *policer-name*	Use policer for the policy data flow for bit-rate limiting and reshaping, check the link for more infomaiton: [bit-Rate Limitation and reshaping function configuration](#) policer-name: policer name, max 16 characters
5	**TRUST** [*cos* / *dscp* / *ip-precedence*]	Policy TRUST status, default use DSCP *cos*: set switch TRUST CoS status *dscp*: set switch TRUST DSCP status

		ip-precedence: set switch TRUST IP priority
6	**set** {**ip dscp** *new-dscp*	**ip precedence** *new-precedence*	**cos** *new-cos* }	Set new value for data flow *new-dscp*: DSCP value, 0-63; *new-precedence*: IP priority value, 0-7 *new-cos*: set CoS value, 0-7
7	**set vlan** *<1-4094>*	Set VLAN override
8	**redirect-to port** *to-port*	Redirect the ports to-port: redirect the ports numbers
9	**copy-to-mirror**	Data flow mirror image
10	**exit**	Return to config-pmap mode
11	**exit**	Return to global configuration mode
12	**exit**	Return to privilege mode
13	**show policy-map** [*WORD*]	Display POLICY MAP information *WORD*: policy map name，max 16 characters

Attention:

➢ So far, policy TRUST (TRUST command) functions are not supported
➢ Set command and policy TRUST command are mutually exclusive.
➢ In one class-map, set command can only be configured in one. Later configuration will take effect

Configuration examples:

Raisecom#**config**

Raisecom(config)#**policy-map** *aaa*

Raisecom(config-pmap)#**class-map** *aaa*

Raisecom(config-pmap-c)#**police** *aaa*

Raisecom(config-pmap-c)#**set cos** *6*

Raisecom(config-pmap-c)#**set ip dscp** *5*

Raisecom(config-pmap-c)#**set ip precedence** *4*

Raisecom(config-pmap-c)#**set vlan** *10*

Raisecom(config-pmap-c)#**redirect-to port** *3*

Raisecom(config-pmap-c)#**exit**

Raisecom(config-pmap)#**exit**

Raisecom(config)#**exit**

Raisecom# **show policy-map** *aaa*

Show as:

 Policy Map aaa

  Class aaa

   police aaa

   set ip precedence 4

set vlan 10

redirect-to port 3

To delete or modify data flow actions:

Steps	Command	Description
1	**Config**	Entry into global configuration mode
2	**policy-map** *policy-name*	Entry into config-pmap mode *policy-name*: policy map name,max 16 characters
3	**class-map** *class-name*	Encapsulate class-map aaa into policy aaa，and entry into config-pmap-c mode *class-name:* class-map name, max 16 characters
4	**no police** *policer-name*	Apply policer in this policy data flow *policer-name*: policer name, max 16 characters
5	**no TRUST** [*cos / dscp / ip-precedence*]	Data flow TRUST status, default use DSCP *cos*: set switch as TRUST CoS status *dscp*: set switch as TRUST DSCP status *ip-precedence*: set switch as TRUST IP priority status
6	**no set** {*ip dscp*/*ip precedence*/*cos*}	Set new value for data flow *new-dscp*: DSCP value, 0-63; *new-precedence*: IP priority value, 0-7 *new-cos*: set CoS value, 0-7
7	**no set vlan**	Set VLAN override
8	**no redirect-to port**	Redirect to port
9	**no copy-to-mirror**	Data flow mirror image
10	**exit**	Return to config-pmap mode
11	**exit**	Return to global configuration mode
12	exit	Return to privilege mode
13	**show policy-map [WORD]**	Display POLICY MAP WORD: policy map name，max 16 characters

Attention: It is not allowed to modify the action if its policy-map has been applied for other ports

23.5.2.4   Apply policy service-policy in ports

It actually does not take effect after all data flow and policy defined. They need to be applied for the ports. The steps for the apply policy are as below:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**service-policy** *policy-name* **ingress** *portid* [**egress** *portlist*]	Apply policy on in/out port.

		policy-name: policy map name, max 16 characters
		portid: in port number
		portlist: out port list
3	**exit**	Return to privilege mode
4	**show policy-map port [***portlist* **]**	Display port policy application information
		portlist: port number

Attention:

➢ QoS must start before appling policy;
➢ When the configuring data flow becomes big, it may fail because it may get the biggest rule of capacity based on those 256 rules for 8 ports.
➢ The TRUST status are mutually exclusive if the TRUST status of the applied front port is not UNTRUST status. After applied, the status will become UNTRUST status.

Application examples:

Raisecom#**config**

Raisecom(config)#**service-policy** *aaa* **ingress** *2* **egress** *1-5*

Raisecom(config)#**service-policy** *bbb* **egress** *1*

Raisecom(config)#**exit**

Raisecom#**show policy-map port**

Display as:

port 2 on ingress:

Policy Map aaa:

Egerss:1-5

Class Map :aaa (match-all)

port 1 on egress:

Policy Map bbb:

23.5.3 Monitoring and Maintenance

Command	Description
show policy-map [*WORD***]**	Display POLICY MAP information
	WORD: policy map name，max 16 characters
show policy-map class {*WORD***}**	Display some classified information of POLICY MAP
	WORD: class-map name，max 16 characters
show policy-map port [*portlist* **]**	Display port policy application information
	portlist: port numbers

1. Display QoS policy-map information

Raisecom#**show policy-map**

Policy Map aaa

    Class aaa

        police aaa

        set ip precedence 4

    Class bbb

        police aaa

To display the specifi name of policy-map information:

Raisecom#**show policy-map** *aaa*

  Policy Map aaa

    Class aaa

        police aaa

        set ip precedence 4

    Class bbb

        police aaa

2. Display some classified information of POLICY MAP

If wanted to show specific policy-map name、indicated class-map name information：

Raisecom#**show policy-map** *aaa* **class-map** *aaa*

  Policy Map aaa

    Class aaa

        police aaa

        set ip precedence 4

3. Display QoS policy-map application information

If wanted to check which policy-map information applied on which ports:

Raisecom#**show policy-map port** *1*

port 1:

  Policy Map aaa:

    Egerss:1-5

        Class Map :aaa (match-all)

        Class Map :bbb (match-all)

If wanted which policy-map information applied on all ports:

Raisecom#**show policy-map port**

port 1:

  Policy Map aaa:

Egerss:1-5

    Class Map :aaa (match-all)

    Class Map :bbb (match-all)

23.5.4 Specific Configuration Examples:

Raisecom#**config**

//Define ACL

Raisecom(config)# **ip-access-list** *1* **permit ip** *10.0.0.2 255.255.255.0 10.0.0.3 255.255.255.0*

Raisecom(config)# **ip-access-list** *2* **permit ip** *10.0.0.3 255.255.255.0 10.0.0.2 255.255.255.0*

//classify data flow

Raisecom(config)# **class-map** *aaa* **match-all**

Raisecom(config-cmap)#**match ip-access-list** *1*

Raisecom(config-cmap)# **exit**

Raisecom(config)# **class-map** *bbb* **match-all**

Raisecom(config-cmap)#**match ip-access-list** *2*

Raisecom(config-cmap)# **exit**

//bit-rate limitation and reshapeing definition, details see：bit-Rate Limitation and reshaping function configuration

Raisecom(config)#**mls qos class-policer** *p-aaa 4000 100* **exceed-action** *drop*

Raisecom(config)# **mls qos class-policer** *p-bbb 8000 200* **exceed-action** *drop*

//define policy

Raisecom(config)#**policy-map** *wmj*

Raisecom(config-pmap)#**class-map** *aaa*   //define data flow classification aaa in policy

Raisecom(config-pmap-c)# **set ip dscp** *5*   //define policy action---set IP DSCP

Raisecom(config-pmap-c)#**police** *p-aaa*   //define policy action——bit-rate limited reshaping

Raisecom(config-pmap-c)#**exit**

Raisecom(config-pmap)#**class-map** *bbb*   //define data flow bbb in policy

Raisecom(config-pmap-c)# **set ip dscp** *6*   //define policy action——set IP DSCP

Raisecom(config-pmap-c)#**police** *p-bbb*   //define policy action——bit-rate limited reshaping

Raisecom(config-pmap-c)#**exit**

Raisecom(config-pmap)#**exit**

Raisecom(config)#**mls qos**

Raisecom(config)#**service-policy** *wmj* **ingress** *1* **egress** *2*　　//apply policy in ports

23.6 Bit-Rate Limitation and Reshaping Function Configuration

23.6.1 Bit-Rate Limitation and Reshaping Default Configuration

None

23.6.2 Configuration Based on Bit-Rate and Reshaping of Data Flow

Create policer as following steps:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**mls qos single-policer** *policer-name rate burst* **exceed-action {drop | policed-dscp-transmit** *marked-dscp* **}**	Create policer in type of single *policer-name*: set policer name *rate*: bit-rate value (Kbps), 8－2000000 *burst:* Burst value (KBps), 8－512000 *drop*: droped packets once it is over bit-rate value *policed-dscp-transmit*: modified DSCP value once it is over bit-rate value *marked-dscp*: modified DSCP value once it is over bit-rate value
3	**mls qos class-policer** *policer-name rate burst* **exceed-action {drop | policed-dscp-transmit** *marked-dscp* **}**	Create policer as type of class *policer-name*: set policer name *rate*: bit-rate value(Kbps), 8－2000000kbps *burst*: burst value (KBps), 8－512000 *drop*: droped packets once it is over bit-rate value *policed-dscp-transmit*: modify DSCP once it is over bit-rate value *marked-dscp*: modified DSCP value once over bit-rate value
4	**mls qos aggregate-policer** *policer-name rate burst* **exceed-action {drop | policed-dscp-transmit** *marked-dscp* **}**	Create policer as type of aggregate *policer-name*：set policer name *rate*: bit-rate value(Kbps), 8－2000000kbps *burst:* burst value (KBps), 8－512000 *drop*: droped packets once it is over bit-rate value *policed-dscp-transmit*: modify DSCP once it is over bit-rate value *marked-dscp*: modified DSCP value once over bit-rate value
5	**exit**	Return to global configuration mode
6	**show mls qos policer** *[single-policer |*	Display policer information

Command	Description
class-policer | aggregate-policer]	*single-policer*: display single policer
	class-policer: display class policer
	aggregate-policer: display aggregate policer

To delete a policer, use command no, **no** {*single-policer/class-policer/aggregate-policer*} *placer-name*.

Attention: When delete a policer, it is not allowed to delete it if its policy is applied for other ports.

23.6.3 Monitering and Maintenance

Command	Description
show mls qos policer [*single-policer | class-policer | aggregate-policer*]	Display policer information *single-policer*: Display single policer *class-policer*: Display class policer *aggregate-policer*: display aggregate policer

Raisecom#**show mls qos policer**

single-policer aaa   44   44   exceed-action policed-dscp-transmit   4

 Used by policy map aaa

To show which port is using policer，use the commands below：

Raisecom#**show mls qos port policers**

Port id 1

policymap name: aaa

policer type: Single, name: aaa

rate: 44 kbps, burst: 44 kbyte, exceed action: policed-dscp-transmit, dscp:4

23.6.4 Specific Configuration Examples

Configuration examples:

Raisecom#**config**

Raisecom(config)# **mls qos single-policer** *aaa 44 44* **exceed-action policed-dscp-transmit** *4*

Raisecom(config)# **exit**

Raisecom#**show mls qos policer**

Display results as:

single-policer aaa 44 44 exceed-action policed-dscp-transmit 4

 Not used by any policy map

If aaa is applied for a port:

Raisecom#**show mls qos port policers**

Port id 1

policymap name: aaa

    policer type: Single, name: aaa

    rate: 44 kbps, burst: 44 kbyte, exceed action: policed-dscp-transmit, dscp: 4

23.7 Map Function Configuration

23.7.1 Map Default Configuration

COS-DSCP default configuration relationship as:

CoS value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

IP-Precedence-DSCP default map relation as:

ToS value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

DSCP-COS default map relation as:

DSCP value	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS value	0	1	2	3	4	5	6	7

DSCP-to-DSCP-Mutation default map relation (default-dscp) as:

DSCP value	0	1	2	3	4	5	6	7
0	8	9	10	11	12	13	14	15
1	16	17	18	19	20	21	22	23
2	24	25	26	27	28	29	30	31
3	32	33	34	35	36	37	38	39
5	40	41	42	43	44	45	46	47
6	48	49	50	51	52	53	54	55
7	56	57	58	59	60	61	62	63

Internal COS – queuing default map relation as:

Internal CoS value	0	1	2	3	4	5	6	7
Queuing ID	1	1	2	2	3	3	4	4

23.7.2 CoS-DSCP map List Configuration

CoS-DSCP map list maps incoming packet COS value as a DSCP value. QoS is used to describe data flow priority. It default map relation as:

CoS value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

To modify the map relations, the following steps are set:

Steps	Commands	Description
1	**config**	Entry into global configuration mode
2	**mls qos map cos-dscp** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	Set new map relation Dscp1-8：DSCP value
3	**exit**	Return to privilege mode
4	**show mls qos maps cos-dscp**	Show QoS COS-DSCP map list

Configuration examples:

Configuration cos-dscp map as 2 3 4 5 6 7 8 9:

Raisecom#**config**

Raisecom(config)# **mls qos map cos-dscp** *2 3 4 5 6 7 8 9*

Raisecom(config)#**exit**

Raisecom# **show mls qos maps cos-dscp**

Show results as:

> *Cos-dscp map:*
>
>   *cos: 0   1   2   3   4   5   6   7*
>
> ---
>
>   *dscp: 2   3   4   5   6   7   8   9*

To backup COS-DSCP map list to default map relation,use command **no**.

Steps	Command	description
1	**config**	Entry into global configuration mode
2	**no mls qos map cos-dscp**	Backup to default map relation
3	**exit**	Return to privilege mode
4	**show mls qos maps cos-dscp**	Display QoS COS-DSCP map list

Raisecom#**show mls qos maps cos-dscp**

> *Cos-dscp map:*
>
>   *cos: 0   1   2   3   4   5   6   7*
>
> ---

dscp: 0   8   16   24   32   40   48   56

23.7.3 IP-Procedence-DSCP Map List Configuration

IP-Procedence-DSCP map-list configuration maps incoming packet ToS into a DSCP value. QoS is used to describe the data flow priority. Its default map relation as show below:

ToS value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

To modify that map relation, set as the following steps:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**mls qos map ip-prec-dscp** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	Set new map relationship Dscp1-8：DSCP value
3	**exit**	Return to privilege mode
4	**show mls qos maps ip-prec-dscp**	Display QoS IP-Procedence-DSCP map list

Configuration example:

Configure ip-prec-dscp map as 2 4 6 8 10 12 14 16:

Raisecom#**config**

Raisecom(config)# **mls qos map ip-prec-dscp** *2 4 6 8 10 12 14 16*

Raisecom(config)#**exit**

Raisecom# **show mls qos maps ip-prec-dscp**

Show results as:

Ip Precedence-dscp map:

ipprec: 0   1   2   3   4   5   6   7

--

dscp: 2   4   6   8   10   12   14   16

Backing up IP-Procedence-DSCP map list to default map relation，use command **no**.

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**no mls qos map ip-prec-dscp**	Backup to default map relation
3	**Exit**	Return to privilege mode
4	**show mls qos maps ip-prec-dscp**	Show QoS IP-Procedence-DSCPmap list

Raisecom#**show mls qos maps ip-prec-dscp**

Ip Precedence-dscp map:

ipprec: 0   1   2   3   4   5   6   7

----

dscp: 0   8   16   24   32   40   48   56

23.7.4 DSCP-CoS Map List Configuration

DSCP-CoSmap list maps the incoming packet DSCP value into a cos value. QoS use its description data flow priority. The default map relation is:

DSCP value	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS value	0	1	2	3	4	5	6	7

To modify that map relation, follows the steps below:

Steps	Command	Description
1	**Config**	Entry into global configuration mode
2	**mls qos map dscp-cos** *dscplist* **to** *cos*	set new map relation Dscplist： DSCP list Cos： cos value
3	**Exit**	Return to privilege mode
4	**show mls qos maps dscp-cos**	Show QoS DSCP- CoSmap list

Configuration examples:

configure **dscp-cos** map, mapping 1-10 into 7:

Raisecom#**config**

Raisecom(config)# **mls qos map dscp-cos** *1-10* **to** *7*

Raisecom(config)#**exit**

Raisecom# **show mls qos maps dscp-cos**

show results as:

Dscp-cos map:

d1 : d2   0   1   2   3   4   5   6   7   8   9

----

0 :   0   7   7   7   7   7   7   7   7   7

1 :   7   1   1   1   1   1   2   2   2   2

2 :   2   2   2   2   3   3   3   3   3   3

3 :   3   3   4   4   4   4   4   4   4   4

4 :   5   5   5   5   5   5   5   5   6   6

5 :   6   6   6   6   6   6   7   7   7   7

6 :   7   7   7   7

Renewing DSCP-CoSmap list to default mapping relation, use command **no:**

steps	command	description
1	**config**	Entry into global configuration mode
2	**no mls qos map dscp-cos**	Back to the default mapping relation
3	**exit**	Return to privilege mode
4	**show mls qos maps dscp-cos**	showQoS DSCP-CoSmap list

Raisecom#**show mls qos maps dscp-cos**

Dscp-cos map:

d1 : d2 0 1 2 3 4 5 6 7 8 9

----

0 :   0 0 0 0 0 0 0 0 1 1

1 :   1 1 1 1 1 1 2 2 2 2

2 :   2 2 2 2 3 3 3 3 3 3

3 :   3 3 4 4 4 4 4 4 4 4

4 :   5 5 5 5 5 5 5 5 6 6

5 :   6 6 6 6 6 6 7 7 7 7

6 :   7 7 7 7

23.7.5 DSCP-MUTATION Map List Configuration

To get the IP data flow with QoS characters in two indepent QoS domain, the ports in the edge of those domains should be set as DSCP TRUST status. Then the receiving port receive the trust DSCP value to avoid QoS classification.   If the DSCP values of those two domains are different, they can be converted through DSCP-to-DSCP converting map list.

DSCP-MUTATIONmap list maps the DSCPvalue into a new DSCP value. QoS uses its description data flow priority. There is a default map listdefault-DSCP in the system and this list could not be modified and deleted.

To modify that mapping relation, set the following steps:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**mls qos map dscp-mutation** *dscpname* *dscplist* **to** *dscp*	Create new DSCP mapping relation Dscpname：DSCP mutation name Dscplist：output port DSCP Dscp：DSCP value
3	**exit**	Return to privilege mode
4	**show mls qos maps dscp-mutation**	showQoS DSCP-MUTATIONmap list

Configuration examples:

Set **dscp-mutation** mapping，map 1-10, 20-30 into 30:

Raisecom#**config**

Raisecom(config)# **mls qos map dscp-mutation** *aaa 1-10* **to** *30*

Raisecom(config)# **mls qos map dscp-mutation** *aaa 20-30* **to** *30*

Raisecom(config)#**exit**

Raisecom# **show mls qos maps dscp-mutation**

Show results as:

Dscp-dscp mutation map:

default-dscp:

d1 : d2   0   1   2   3   4   5   6   7   8   9

---

0 :	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1 :	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*
2 :	*20*	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*	*29*
3 :	*30*	*31*	*32*	*33*	*34*	*35*	*36*	*37*	*38*	*39*
4 :	*40*	*41*	*42*	*43*	*44*	*45*	*46*	*47*	*48*	*49*
5 :	*50*	*51*	*52*	*53*	*54*	*55*	*56*	*57*	*58*	*59*
6 :	*60*	*61*	*62*	*63*						

Dscp-dscp mutation map:

aaa:

d1 : d2   0   1   2   3   4   5   6   7   8   9

---

0 :	*0*	*30*	*30*	*30*	*30*	*30*	*30*	*30*	*30*	*30*
1 :	*30*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*
2 :	*30*	*30*	*30*	*30*	*30*	*30*	*30*	*30*	*30*	*30*
3 :	*30*	*31*	*32*	*33*	*34*	*35*	*36*	*37*	*38*	*39*
4 :	*40*	*41*	*42*	*43*	*44*	*45*	*46*	*47*	*48*	*49*
5 :	*50*	*51*	*52*	*53*	*54*	*55*	*56*	*57*	*58*	*59*
6 :	*60*	*61*	*62*	*63*						

To delete DSCP-MUTATION map list，use command **no**.

steps	command	description
1	**config**	Entry into global configuration mode
2	**no mls qos map dscp-mutation** *dscpname*	Delete DSCP mapping relation Dscpname：DSCP mutation name
3	**exit**	Return to privilege mode
4	**show mls qos maps dscp-mutation**	showQoS DSCP-CoSmap list

To apply the map list for DSCP-mutation，it could be used in port mode. Port default uses default-dscp mapping relation.

steps	command	description
1	**config**	Entry into global configuration mode
2	**interface port** *portid*	Entry into port mode
3	**mls qos dscp-mutation** *dscpname*	Apply DSCP mapping relation *dscpname*: DSCP mutation name, max 16 characters
4	**exit**	Return to configuraton mode
5	**exit**	Return to privilege mode
6	**show mls qos port** *portid*	Show QoS port configuration information

Configuration examples:

Raisecom#**config**

Raisecom(config)#**interface port** *1*

Raisecom(config-port)# **mls qos dscp-mutation aaa**

Raisecom(config-port)# **exit**

Raisecom(config)#**exit**

Raisecom#**show mls qos port** *1*

To check wether the configuration is right, use command show:

Raisecom#**show mls qos port** *1*

port 1:

TRUST state: not TRUSTed

default COS: 0

default DSCP: 0

DSCP override: disable

DSCP Mutation Map: aaa

Attention: In ISCOM2800 series, DSCP-MUTATION map list uses fiter list to get hardware. In hardware, port 1-8 use same filter list (same as 9－16, 17－24, port 25, port 26 are using one filter list individually, 5 filter list in total). Thus, as any port in port 1-8 is using DSCP-MUTATION map list, the rest ports of port 1－8 are using DSCP-MUTATION map list as well.

To decline DSCP-MUTATION map list application in the port，use command **no**.

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**interface port** *portid*	Entry into port mode
3	**no mls qos dscp-mutation** *dscpname*	Decline using DSCP map relation dscpname: DSCP mutation name, max 16 characters
4	**exit**	Return to configuration mode

5	**exit**	Return to privilege mode
6	**show mls qos port** *portid*	showQoS port configuration information

To check whether the configuration is right, use command show:

Raisecom#**show mls qos port** *1*

port 1:

TRUST state: not TRUSTed

default COS: 0

default DSCP: 0

DSCP override: disable

DSCP Mutation Map: default-dscp

Attention: When dscp-mutationmap list is used in some other port，its map list could not be deleted；only the map list is not used, it could be deleted.

23.7.6 CoS-queue Map List Configuration

CoS-queuemap list is sent to the output queue which is decided by the incoming packet CoS value. QoS uses its description data flow priority, and its default map relation is:

Internal CoS value	0	1	2	3	4	5	6	7
Queue ID	1	1	2	2	3	3	4	4

To modify the map relation，set up with the following relation:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**queue cos-map** *queueid coslist*	set new map relation, packets CoS value in 1-4 are sent to Queue 1 Queueid: Queue number Coslist: CoS value
3	**exit**	Return to privilege mode
4	**show mls qos queuing**	Show QoS queue map list

Configuration examples:

Raisecom#**config**

Raisecom(config)# **queue cos-map** *1 1-4*

Raisecom(config)#**exit**

Raisecom#**show mls** *qosqueueing*

show results as:

the queue schedule mode: strict priority(SP)

Cos-queue map:

   cos-queueid

    0 - 1

    1 - 1

    2 - 1

    3 - 1

    4 - 1

    5 - 3

    6 - 4

    7 - 4

To renew CoS-queue map list to default map relation, use command **no**.

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**no queue cos-map**	Renew default map relation
3	**exit**	Return to privilege mode
4	**show mls qos queuing**	Show QoS queuing map list

To check wehter the configuration is correct，use command show:

Raisecom#**show mls** *qos queueing*

  the queue schedule mode: strict priority(SP)

Cos-queue map:

   cos-queueid

    0 - 1

    1 - 1

    2 - 2

    3 - 2

    4 - 3

    5 - 3

    6 - 4

    7 - 4

23.7.7 Set Ports Based on smac, dmac, vlan's Frame Priority and Priority Override Function

Ports can be based on smac、dmac、vlan entering switch's message farme priority and queue priority override.

Configuration steps as below:

Steps	Command	Description
1	**config**	entry into global configuration mode
2	**interface** { port-list } *<1-MAX_PORT_NUM >*	Entry into Ethernet physic interface mode *1-MAX_PORT_NUM* equipement port numbers
3	**mls qos** *{smac | dmac}* *{priority-set|cos-override}*	set up ports based onsmac, dmac's frame priority or queue priority override function Smac: source MAC Dmac: destination MAC *cos-override*: frame priority *priority-set*: queuepriority
4	**mls qos** *{smac|dmac}* *priority-set cos-override*	set up ports based onsmac,dmac's frame priority and queue priority override function Smac: source MAC Dmac: destination MAC *cos-override*: frame priority *priority-set*: queue priority
5	**mls qos vlan** *{priority-set|cos-override}*	set up ports based onvlan's frame priority or queue priority override function *cos-override*: frame priority *priority-set*: queue priority
6	**mls qos vlan** *priority-set cos-override*	set up ports based on vlan's frame priority and queue priority override function *cos-override*: frame priority *priority-set*: queue priority
7	**exit**	Exit
8	**show mls qos port-list** *{1-MAX_PORT_NUM }*	Display QoS configuration information *1-MAX_PORT_NUM* equipement port numbers

To use command no　　Renew all priority override based on smac、dmac、vlanto default configuration(even both of them are not override).

23.7.8 Monitering and Maintenance

Command	Description
show mls qos maps *[cos-dscp | ip-prec-dscp | dscp-cos | dscp-mutation]*	Display all map list's configuration content。 *cos-dscp*: COS to DSCP map *ip-prec-dscp*: Ip priority to DSCP map *dscp-cos*: DSCP to CoS map *dscp-mutation*: DSCP mutation map
show mls qos queuing	Display QoS queue map list

show mls qos port-list *{1-MAX_PORT_NUM }*	Display QoS configuration information *1-MAX_PORT_NUM:* equipement port numbers

1．Map list information maps

Raisecom#**show mls qos maps**

Dscp-cos map:

d1 : d2   0   1   2   3   4   5   6   7   8   9

----

0 :   0   0   0   0   0   0   0   0   1   1

1 :   1   1   1   1   1   1   2   2   2   2

2 :   2   2   2   2   3   3   3   3   3   3

3 :   3   3   4   4   4   4   4   4   4   4

4 :   5   5   5   5   5   5   5   5   6   6

5 :   6   6   6   6   6   6   7   7   7   7

6 :   7   7   7   7

Cos-dscp map:

cos: 0   1   2   3   4   5   6   7

---

dscp: 0   8   16   24   32   40   48   56

Ip Precedence-dscp map:

ipprec: 0   1   2   3   4   5   6   7

---

dscp: 0   8   16   24   32   40   48   56

Dscp-dscp mutation map:

default-dscp:

d1 : d2   0   1   2   3   4   5   6   7   8   9

--

0 :   0   1   2   3   4   5   6   7   8   9

1 :   10   11   12   13   14   15   16   17   18   19

2 :   20   21   22   23   24   25   26   27   28   29

3 :   30   31   32   33   34   35   36   37   38   39

4 :   40   41   42   43   44   45   46   47   48   49

5 :   50   51   52   53   54   55   56   57   58   59

6 :   60   61   62   63

Dscp-dscp mutation map:

aaa:

d1 : d2	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0 :	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1 :	*30*	*30*	*30*	*30*	*30*	*30*	*30*	*30*	*30*	*30*
2 :	*30*	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*	*29*
3 :	*30*	*31*	*32*	*33*	*34*	*35*	*36*	*37*	*38*	*39*
4 :	*40*	*41*	*42*	*43*	*44*	*45*	*46*	*47*	*48*	*49*
5 :	*50*	*51*	*52*	*53*	*54*	*55*	*56*	*57*	*58*	*59*
6 :	*60*	*61*	*62*	*63*						

2． Queue map list information queueing

Raisecom#**show mls qos queueing**

t*he queue schedule mode: bounded delay*

wrr queue weights:

queueid-weights-delay

1 - 1 - 100

2 - 3 - 100

3 - 5 - 100

4 - 7 - 100

Cos-queue map:

cos-queueid

0 - 1

1 - 1

2 - 2

3 - 2

4 - 3

5 - 3

6 - 4

7 - 4

3． display QoS configuration information:

Raisecom#**show mls qos port-list** *2*

port	*smac-policy*	*dmac-policy*	*vlan-policy*
2	*priority-set*	*--*	*--*

23.7.9 Specific Configuration Examples

See the sections for details.

23.8 Queue and Adjust Function Mode

So far, the equipements support four queue adjust modes: strict priority (SP), weighted priority (WRR), BOUND-DELAY mode and SP+WRR's mixed mode. Default set is priority mode.

23.8.1 Queue and Adjust Default Configuration

Function	Default value
Queue adjust policy	Strict priority adjust SP

23.8.2 SP Configuration

Configuration steps as:

Steps	Command	Description
1	**config**	entry into global configuration mode
2	**queue strict-priority**	Configuration is strict priority
3	**exit**	Return to privilege mode
4	**show mls qos queuing**	display QoS queuing information

23.8.3 WRR Configuration

Configuration steps as:

Steps	Command	Description
1	**config**	entry into global configuration mode
2	**queue wrr-weight** *weight0 weight1 weight2 weight3*	Set ports' adjust mode as WRRmode Weight 0-3: set queue 0-3 weight value
3	**exit**	Return to privilege mode
4	**show mls qos queuing**	display QoS queuing information

23.8.4 SP+WRR Configuration

Configuration steps as:

Steps	Command	Description
1	**config**	entry into global configuration mode

2	**queue preemp-wrr** *weight1 weight2 weight3*	Set port adjust mode as PREEMP-WRR mode, like queue1 is strict priority, rest queues follow the weights Weight 1-3: set queue1-3 weight value
3	**queue preemp-wrr** *weight0 weight1*	Set ports adjust mode as PREEMP-WRR mode, like queue 0, 1 are strict priority, rest queue follow the weights
4	**exit**	Return to privilege mode
5	**show mls qos queuing**	display QoS queuing information

23.8.5 Monitering and Maintenance

Command	Description
show mls qos queuing	Display QoS's queuemap list

➢ Queue map list information queueing

Raisecom#**show mls qos queueing**

the queue schedule mode: bounded delay

wrr queue weights:

queueid-weights-delay

1 - 1 - 100

2 - 3 - 100

3 - 5 - 100

4 - 7 - 100

Cos-queue map:

cos-queueid

0 - 1

1 - 1

2 - 2

3 - 2

4 - 3

5 - 3

6 - 4

7 - 4

23.8.6 Specific Configuration Examples

Configuration examples: set queue as WRR mode，weight as 1:2:4:8:

Raisecom#**config**

Raisecom(config)# **queue wrr-weight** *1 2 4 8*

Raisecom(config)#**exit**

Raisecom#**show mls qos queuing**

Display results:

Raisecom#**show mls qos queuing**

the queue schedule mode: weighted round robin(WRR)

wrr queue weights:

Queue ID - Weights - Delay

1 - 1 - 0

2 - 2 - 0

3 - 4 - 0

4 - 8 - 0

23.9 QoS Trouble Shoot

➢ Port TRUST status and policy configuration are mutually exclusive.
➢ Data flow TRUST status and SET actions are mutually exclusive.
➢ To delete class-map、policy-map、policer，it will be failed if they have been applied for the ports.
➢ If class-map、policy-map have been applied for the ports, then modification for match statements and data flow actions (as set action) will fail.
➢ Before apply data flow policy, QoS must be started first; data flow policy will be failed if QoS is stopped.
➢ If class-map match type is matcha-all, the configuration may fail because there might be conflicts between matching information.
➢ To match a ACL, ACL must be defined first and its type must be permit.
➢ To match a class-map, sub class-map must be type of match-all.
➢ As configuration data flow become more, it may be failed in applying because it is getting the capacity biggest rule. (8 ports have 256 rules)
➢ To start QoS policy, it is suggested to turn off data flow control function;

23.10 QoS Command Reference

Command	Description
[no] mls qos	Run and Stop QoS
[no] mls qos trust [cos | dscp | ip-precedence]	Set ports TRUST status
mls qos default-cos *default-cos*	Set QoS ports Default CoS value
no mls qos default-cos	Renew QoS ports Default CoS value
mls qos map dscp-mutation *dscp-name dcp-list* **to** *dscp*	Create DSCP-mutaion map list
no mls qos map dscp-mutation *dscp-name*	Delete DSCP-mutaion map list
[no] mls qos dscp-mutation *dscp-name*	Apply or decline DSCP-mutaion map application
class-map *class-map-name* **[match-any | match-all]**	Create class-map

no class-map *class-map-name*	Delete class-map
[no] policy-map *policy-map-name*	Create delete policy map
description *WORD*	Set policy map and class-map description information
[no] class *class-map-name*	apply class map on policy
match { **ip-access-list** *acl-index* | **mac-access-list** *acl-index* | **access-list-map** *acl-index* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list* | **class** *calss-name* | **vlan** *vlanlist*}	Set match statements
no match { **ip-access-list** *acl-index* | **mac-access-list** *acl-index* | **access-list-map** *acl-index* | **ip dscp** | **ip precedence** | **class** *calss-name* | **vlan** *vlanlist* }	Delete match statements
[no] trust [**cos** | **dscp**]	Set data flow TRUST status
set {**ip dscp** *new-dscp* | **ip precedence** *new-precedence* | **cos** *new-cos* }	Set actions
no set {**ip dscp** | **ip precedence** | **cos** }	Delete set value
mls qos {**aggregate-policer** |**class-policer** | **single-policer** } *policer-name rate burst* [**exceed-action** { **drop** | **policed-dscp-transmit** *dscp* }]	Create policer
no mls qos {**aggregate-policer** |**class-policer** | **single-policer** } *policer-name*	Delete policer
[no] police *policer-name*	Apply policer
service-policy *policy-map-name* **ingress** *portid* [**egress** *portlist*]	Apply policy
no service-policy *policy-map-name* **ingress** *portid*	Decline apply policy
mls qos map cos-dscp *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	configurationCoS to DSCP map
no mls qos map cos-dscp	Renew CoS to DSCP map
mls qos map ip-prec-dscp *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	Configuration ToS to DSCP map
no mls qos map ip-prec-dscp	Renew ToS to DSCP map
mls qos map dscp-cos *dscp-list* **to** *cos*	Configuration DSCP to switch internal priority map
no mls qos map dscp-cos	Renew DSCP to switch internal priority map
queue cos-map *queue-id cos-list*	Configuration switch internal priority to queue map
no queue cos-map	Renew switch internal priority to queue map
queue wrr-weight *weight0 weight1 weight2 weight3*	Configuration switch queue adjust mode as WRR
queue bounded-delay *weight0 weight1 weight2 weight3 delaytime*	Set port adjust mode as BOUNDDELAY mode
queue preemp-wrr *weight1 weight2 weight3*	Set port adjust mode as PREEMP-WRR mode

queue strict-priority	Set port adjust mode as strict priority mode
show mls qos	Display QoS on/off status
show mls qos policer [*policename | aggregate-policer |class-policer | single-policer* **]**	Display policer information
show mls qos maps [*cos-dscp | dscp-cos | dscp-mutation | ip-prec-dscp*]	Display every map list configuration content
show mls qos queueing	Display in/out queue configuration information
show mls qos port *portid* [**policers**]	Display port strategy configuration，policer,etc information
show class-map [*class-map-name*]	Display class-map information
show policy-map [*policy-map-name* | [**port** *portId*] [**class** *class-name*]	Display policy information

Chapter 25 802.3ah OAM

24.1 802.3ah OAM Principle Introduction

IEEE802.3ah OAM (Operation Administration Maintenance) is used to provide more efficient Ethernet link operation, management and maintenance. As the efficient complimentarity of the high managing tool, OAM enhances the Ethernet management and monitoring.

24.1.1 OAM mode

The process of Ethernet OAM connecting is also called Discovery, which is the process of one OAM entity discovers another one in the remote device for creating a stable conversation.

In the process, the connected Ethernet OAM (OAM Function port) entity sends the Ethernet configuration information and local node support Ethernet OAM ability information by switching the information OAM PDU to the opposite in two way. Once OAM receives the configuration data from the opposite, it will decide whether build the OAM connection up. If both ends are agreed to build up the OAM connections, Ethernet OAM protocol will start to run on the LAN Layer.

There are two modes for building up Ethernet OAM connection: active mode and passive mode. The connection can only be active by OAM entity and passive OAM entity has to wait for the connecting request from the opposite OAM entity.

After the Ethernet OAM is connected, OAM entities from both ends send information OAMPDU to keep the connection. If the Information OAMPDU is not received by the OAM entity from opposite in 5 seconds, it will be considered as connection time-out. Thus OAMs are needed to reconnect.

Information OAMPDU packet is sent by internal counter control with maximum rate of 10 packets/second.

24.1.2 OAM loop-back

OAM loop-back can only be achieved after Ethernet OAM connection is built up。 In connected situation，active mode OAM will send OAM loop-back command and opposite will response for that command. As remote is in loop-back mode，all packets but OAMPDU packet will be sent back in the original route.

Periodical loop-back detection can detect network failure on time and find out the failure happened location by subsection loop-back detection. It can help users to remove failure.

24.1.3 OAM events

It is difficult to detect the Ethernet failure，especially when the physical network communicational is in no-breakdown but low network. OAMPDU states a Flag Domain which allows Ethernet OAM entity sends the failure information to the opposite. That Flag also states the threshold events as shown below:

Link Fault: Signal lost in the opposite link.

Dying Gasp: Unpredict states happen, as power cut-down.

Critical Event：Uncertain critical events happen.

Ethernet OAM connecting process is continually sending the Information OAMPDU. Local OAM entity can send the local threshold event information to opposite OAM entity through Information OAMPDU. The Administrators can always notice the link status and solve the related problems on time.

Ethernet OAM　monitors the link by Event Notification OAMPDU switchs。Once the link fails, the local link will monitor the failure. And it will send monitors the Event Notification OAMPDU to opposite Ethernet OAM entity to inform the threshold events. Administrator can notice the network status by monitoring the link.

 - ➢ Error frame event：error frame number in unit time is over stated threshold number.
 - ➢ Error frame period event：states frame number N as a period; it means in the period of received N error frames, the error fame number is over stated threshold one.
 - ➢ Error frame second event: indicated in M seconds, the error frame's time in seconds are over the stated threshold number.(error frame second states: an error frame happens in a specific second and this second is called error frame second.)

24.1.4 OAM mib

Devices can gain opposite device link configuration/ statistics value through OAM and then get link status/ data.

24.2 802.3ah OAM Mode Configuration

OAM supports two modes: active mode and passive mode. Active mode starts OAM opposite discover process, supports functions but non-response remote loop-back command and variable gained requests; passive mode does not start OAM opposite discover process, does not send remote loop- back command and veriable gained request. Different devices use different mode supports and default configurations. If the device supports passive mode, then its default mode will be passive mode or it will be active mode. If the device only supports one mode, then it does not support mode configuration. OAM mode. OAM mode is all OAM port link share, and users can set mode configuration on the devices which support both two mode as shown below:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**oam** *{active/passive}*	Set OAM as active/passive mode
3	**Exit**	Return to privilege use mode
4	**show oam**	Show OAM loop-back information

Set device OAM as active mode：

Raisecom#**config**

Raisecom(config)#**oam** *active*

Raisecom(config)#**exit**

Raisecom#**show oam**

24.3 802.3ah OAM Active Mode Function

24.3.1 OAM default configuration

Function	Default Value
OAM Enable\Disable	Enable
Opposite OAM event alarm	Disable

24.3.2 OAM enable/disable configuration function

✧   OAM Enable\Disable

OAM is Ethernet point to point link protocal. Enable/Disable is used for all the link ports. In default situation, all ports OAM are Enable, user can Enable/ Disable OAM by the following steps:

Steps	Command	Description
1	**Config**	Entry global configuration mode
2	**interface port** *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**oam** {*disable* / *enable*}	Enable or Disable OAM
4	**Exit**	Return Global Configuration mode
5	**Exit**	Return privileged EXEC mode
6	**show oam**	Show OAM Configuration state

Disable port 2 OAM:

Raisecom#**config**

Raisecom(config)#**interface port** *2*

Raisecom(config-port)#**oam** *disable*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

✧   Show OAM local link status

Privilege mode command: show oam can display OAM link local configuration and status include mode configuration, management status, working status, maximum packet length, configuration version and function support , etc. Through this command, users can understand OAM link configuration, running status, etc.

Raisecom#**show oam**

Port: 1

Mode: Passive

Administrate state: Enable

Operation state: Disabled

Max OAMPDU size: 1518

Config revision: 0

Supported functions: Loopback, Event, Variable

Port: 2

Mode: Passive

Administrate state: Disable

Operation state: Disable

Max OAMPDU size: 1518

Config revision: 0

Supported functions: Loopback, Event, Variable

✧ Show OAM opposite link status

Privilege mode command: show oam peer can display the opposite device information on OAM link, include: opposite MAC address, manufactory OUI, manufactory information, mode configuration, maximum packet length, configuration version and function support information. If OAM link is not connected, then there no information will be displayed.

Raisecom#**show oam peer**

Port: 1

Peer MAC address: 000E.5E00.91DF

Peer vendor OUI: 000E5E

Peer vendor info: 1

Peer mode: Active

Peer max OAMPDU size: 1518

Peer config revision: 0

Peer supported functions: Loopback, Event

24.3.3 Run OAM loop-back function

OAM provide link layer remote loop-back system, which can be used for located link error position, performance and quality test. Under link loop-back status, devices will loop-back all link received packets to the opposite devices except OAM packet. Local device uses OAM remote command to enable or disable remote loop-back. Opposite device will use loop-back configuration command to control whether response loop-back command.

In central office end , users can build up remote loop-back through remote loop-back command.

Steps	Command	Description

1	**config**	Entry global configuration mode
2	**interface port** *port_number*	Entry Ethernet physical interface mode, *port_number* is physical interface number
3	**oam remote-loopback**	Build up remote loop-back
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam loopback**	Show OAM loop-back situation

Build remote loop-back on port link 2:

Raisecom#**config**

Raisecom(config)#**interface port** *2*

Raisecom(config-port)#**oam remote-loopback**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show oam loopback**

Users can remove remote loop-back as below:

Steps	Command	Description
1	**Config**	Entry global configuration mode
2	**interface port** *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**no oam remote-loopback**	Remove remote loop-back
4	**Exit**	Return global configuration mode
5	**Exit**	Return privileged EXEC mode
6	**show oam loopback**	Show OAM loop-back state

Remote loop-back on remove end link 2：

Raisecom#**config**

Raisecom(config)#**interface port** *2*

Raisecom(config-port)#**no oam remote-loopback**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show oam loopback**

Note: Remote loop-back only can be achieved after Ethernet OAM is connected.

24.3.4 Opposite OAM event alarm function

By default, when opposite link monitor event is received, device will not inform network managing center through SNMP TRAP. Users can use Enable/Disable opposite monitor events is informed to the network managing center.

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface port** *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**oam peer event trap** *{disable | enable}*	Enable or Disable opposite OAM monitor event is informed network managing center
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam trap**	show OAM TRAP information

Enable port 2 opposite link monitoring event informed to network managing center:

Raisecom#**config**

Raisecom(config)#**interface port** *2*

Raisecom(config-port)# **oam peer event trap** *enable*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show oam trap**

24.3.5 View opposite IEEE 802.3 Clause 30 mib

OAM variable gain is a link monitoring measure. It allows local device to get opposite device current variable value thus get current link status. IEEE802.3 Clause30 particulary states the variables which support OAM gain and their representing way. Variable can be divided into its biggest unit -- object which include package and attribute. Package also is combined by sereval attribute. Attribute is variable's smallest unit. OAM variable gain uses Clause 30 to state object/package/attribute's branch described requesting objects. And branches plus the variable value are used to represent object response variable request. Now，all devices have supported both OAM information and port statistics as object variable gain. EPON OLT device also supports MPCP and OMPEmulation object information gain.

When device OAM work as active mode, users can gain opposite devices OAM information or port statistics variable values as the steps below:

Steps	Command	Description
1	**show oam peer** *{link-statistics | oam-info} {port-list | client | line} port_number*	Gain opposite device OAM information or port statistics variable value *port_number* is physical interface number

Gain port 2 opposite device OAM information value is shown as below:

Raisecom(debug)#**show oam peer oam-info port-list** *2*

Note: OAM variable gain is only achieved if and only if Ethernet OAM connection is built up.

24.3.6 OAM statistics clear function

OAM calculates the number of all different types of OAM packets which are sent/received on each OAM port link. The types of packets are：information，link event information，loop-back control，variable gain request，variable gain response，organise using，uncertain type and repeated event information. Users can clear port link OAM statistics information as follow steps:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface port** *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**clear oam statistics**	Clear OAM port link statistics information
4	**exit**	Entry global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam statistics**	show OAM link statistics information

Clear port 2 OAM link statistics information as below:

Raisecom#**config**

Raisecom(config)#**interface port** 2

Raisecom(config-port)#**oam clear statistics**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show oam statistics**

24.3.7 Monitoring and maintenance

Command	Description
show oam	show OAM link's local configuration and status
show oam peer	show OAM link's opposite device information
show oam loopback	Show remote loop-back information
show oam peer event	show opposite device informed event
show oam trap	Show OAM related SNMP TRAP information and its configuration situation.

show oam statistics	show all OAM port link statistics information

24.3.8 Configuration example
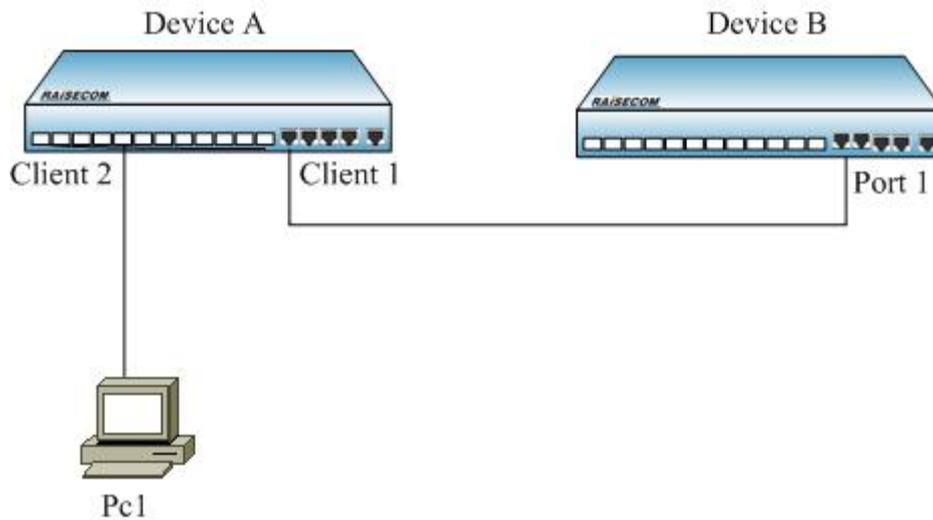
Figure 1-1

As figure 1-1, to set remote loop-back as following configuration:

Raisecom#**config**

Raisecom (config)#**interface port** *1*

Raisecom(config-port)#**oam** *enable*

Raisecom(config-port)#**exit**

Raisecom#**show oam port-list** *1*

   Port: 1

   Mode: Active

   Administrate state: Enable

   Operation state: Operational

   Max OAMPDU size: 1518

   Config revision: 0

   Supported functions: Loopback, Event

Raisecom#**config**

Raisecom (config)#**interface port** 1

Raisecom(config-port)#**oam remote-loopback**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show oam loopback**

   Port: 1

   Loopback status: Remote

Loopback react: Ignore

24.4 802.3ah OAM Passive Function

24.4.1 OAM default configuration

Function	Default Value
Oam Enable\Disable	Enable
Oam mode	Passive
Response\Ignore opposite oam loop-back Configuration	Response
Local oam event alarm	Disable
Oam failure indication	Enable
Error frame periodical event window and threshold.	window 10 (s) Threshold 1 (unit)
Error frame event window and threshold	Window 10 (s) Threshold 1 (unit)
Error frame second statitics event window and threshold	Window 600 (s) Threshold 1 (unit)

24.4.2 OAM enable/disable configuration

> OAM Enable\Disable

OAM is Ethernet point to point link protocal, Enable/Disable is for different link port. In default situation, all ports OAM are Enable. Users can enable/disable OAM by following steps:

Steps	Command	Description
1	**Config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**oam** {**disable** | **enable**}	Enable or Disable OAM
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode
6	**show oam**	show OAM configuration situation

Disable port 2 OAM as follow:

Raisecom#**config**

Raisecom(config)#**interface port** *2*

Raisecom(config-port)#**oam** *disable*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

> ➢ Show OAM local link status

Privileged EXEC mode command: show oam can show OAM link local configuration and status, displayed information is include mode configuration, managing status，running status，maximum packet length, configuration version and function support information. By this command, users can understand OAM link configuration, running status such information.

Raisecom#**show oam**

Port: 1

Mode: Passive

Administrate state: Enable

Operation state: Disabled

Max OAMPDU size: 1518

Config revision: 0

Supported functions: Loopback, Event, Variable

Port: 2

Mode: Passive

Administrate state: Disable

Operation state: Disable

Max OAMPDU size: 1518

Config revision: 0

Supported functions: Loopback, Event, Variable

> ➢ Show OAM opposite link status

Privileged EXEC mode command: show oam peer can show OAM link's opposite device information, include opposite MAC address, manufactory OUI, manufactory information, mode configuration, maximum packet length, configuration version and function support information. If OAM link is not built up, then it will not show any information.

Raisecom#**show oam peer**

Port: 1

Peer MAC address: 000E.5E00.91DF

Peer vendor OUI: 000E5E

Peer vendor info: 1

Peer mode: Active

Peer max OAMPDU size: 1518

Peer config revision: 0

Peer supported functions: Loopback, Event

24.4.3 Response/ignore opposite OAM loop-back configuration function

OAM provide link layer remote loop-back system, can be used for locating link error position, function and quality testing. In link loop-back status, all packets received from the link but OAM packet loop-back to opposite device. Local device use OAM remote loop-back command enable or disable remote loop-back, opposite device uses loop-back configuration command control to response loop-back command.

In default situation，device loop-back responses as Enable, users set loop-back response configuration as below:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**oam loopback** {**ignore** | **process**}	Enable or Disable OAM loop-back response
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam loopback**	show OAM loop-back situation

Disable response port link 2 OAM remote loop-back：

Raisecom#**config**

Raisecom(config)#**interface port** *2*

Raisecom(config-port)#**oam loopback ignore**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show oam loopback**

24.4.4 OAM link monitor configuration function

OAM link monitor is used to detect and report different link errors. When link errors are detected, device informs opposite error cause time, window and threshold configuration by OAM event information packets. Opposite reports events to network managing center by SNMP TRAP. Local device reports events directly to network managing center by SNMP TRAP. OAM link monitoring supports events below:

Error frame events: indicates periodical error frames over threshold. When indicated time periodicaly error frames over threshold, device will have that event.

Error frame periodical event: lately N frames' error are over threshold, N is indicated value; once laterly N frames' error over threshold is detected, device will release that event.

Error frame second statistics event: lately M seconds, the error frams' second number over threshold. M is the indicated value. When error frame second number is over indicated threshold in M seconds, device releases that event.

OAM named the previous monitoring period, frame calculate number and second statistics number as

monitoring window.

Users can set the link monitoring configuration as steps below:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Enter Ethernet physical interface mode *port_number* is physical interface number
3	**oam errored-frame window** *<1-60>* **threshold** *<0-65535>*	Config error frame monitoring window and threshold *<1-60>* is monitoring window，unit is second, *<0-65535>* is threshold.
4	**oam errored-frame-period window** *<100-60000>* **threshold** *<0-65535>*	Config error frame periodical event monitoring window and threshold *<100-60000>* is monitoring window, unit is second, *<0-65535>*is threshold.
5	**oam errored-frame-seconds window** *<10-900>* **threshold** *<0-900>*	Config error frame statistics monitoring window and threshold *<10-900>* is monitoring window, unit is second, *<0-900>* is threshold.
6	**exit**	Return to global configuration mode
7	**exit**	Return to privileged EXEC mode
8	**show oam notify**	show OAM events configuration situation

Configuration port 2 error frame event monitoring window is 2 seconds, threshold is 8 error frame: error frame period event monitoring window is 100 ms, threshold is 128 error frames; error frame second statistics event monitoring window is 100 seconds, threshold is 8 seconds.

Raisecom#**config**

Raisecom(config)#**interface port** *2*

Raisecom(config-port)# **oam errored-frame window** *2* **threshold** *8*

Raisecom(config-port)# **oam errored-frame-period window** *100* **threshold** *128*

Raisecom(config-port)# **oam errored-frame-second window** *100* **threshold** *8*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show oam notify**

Using physical layer interface configuration command **no oam errored-frame** can resume error frame event monitoring window and threshold as Default Value

Using physical layer interface configuration command **no oam errored-frame-period** can resume error frame event monitoring window and threshold as Default Value

Using physical layer interface configuration command **no oam errored-frame-second** can resume error frameevent monitoring window and threshold as Default Value.

24.4.5 OAM fault indication function

OAM fault indication function is used to inform opposite device local device with abnormal event as link-fault, power break, abnormal temperature, etc. Those will cause the faults as link disable, device restart, ect. Now stated faults are link-fault, dying-gasp and critical-event caused by abnormal temperature. In default, device fault indicated as Enable status, thus when fault happened, device informs opposite by OAM. Users can Enable or Disable faults (except link-fault fault indicated must inform opposite) by following steps:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**oam notify** {*dying-gasp* | *critical-event} {disable|enabl*}	Enable or Disable OAM error indicated opposite
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam notify**	show OAM event configration situation

Disable port 3 critical-event fault indication:

Raisecom#**config**

Raisecom(config)#**interface port** *3*

Raisecom(config-port)# **oam notify critical-event** *disable*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show oam notify**

24.4.6 Local OAM event alarm function

In Default, when link monitoring event is detected, device will not inform network managing center by SNMP TRAP. Users can use Enable or Disable to inform network managing center the monitor events by following steps:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**oam event trap** {*disable* | *enable}*	Enable or Disable OAM monitoring event to inform network managing center
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode

	6	**show oam trap**	show OAM TRAP information

Enable port 2 link monitoring event inform to network managing center:

Raisecom#**config**

Raisecom(config)#**interface port** *2*

Raisecom(config-port)# **oam event trap** *enable*

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show oam trap**

24.4.7 IEEE 802.3 Clause 30 mib support

OAM variable gain is a link monitoring measure. It allows local device to gain opposite device lately variable value. Thus it can gain lately link status. IEEE802.3 Clause30 detailly states support OAM gain variable and its representation. Object is the biggest division of variable. Each object has package and attribute. Package is include many attribute. Thus attributes are the smallest variable unit. OAM variable gain states object/package/attribute branches description as request objects，and branches plus variable value are used to represent as object response variable request. Now, all devices can support OAM information and port statistics variable gain. EPON OLT device also supports MPCP and OMPEmulation object information gain.

When device OAM is in active mode，users can gain opposite device OAM information or port statistics variable value by following steps:

Steps	Command	Description
1	**show oam peer** {**link-statistics** | **oam-info**} { **client** | **line**} *port_number*	Gain opposite device OAM informationor port statistics variable value *port_number* is physical interface number

Gain port 2 opposite device OAM information value:

Raisecom(debug)#**show oam peer oam-info port-list** *2*

24.4.8 OAM statistics clear function

OAM statistics sending/receiveing all OAM packets number on each OAM port link. Packets types:information，link events information, loop-back control，variable gain request，variable gain response，organise using，uncertain type and repeat event inforamtion. Users can clear port link OAM statistics information as following steps:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number

	3	**clear oam statistics**	Clear OAM port link statistics information
	4	**exit**	Return to global Configuration mode
	5	**exit**	Return to privileged EXEC mode
	6	**show oam statistics**	show OAM link statistics information

Clear port 2 OAM link statistics information

Raisecom#**config**

Raisecom(config)#**interface port** 2

Raisecom(config-port)#**oam clear statistics**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show oam statistics**

OAM record recent happening local and opposite link monitoring and fault (key) events. Users can clear port link OAM local and opposite events record as following steps:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**clear oam event**	Clear OAM port link event record
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam event**	show OAM link local event record
7	**Show oam peer event**	show OAM link opposite event record

Clear port 2 OAM link events record:

Raisecom#**config**

Raisecom(config)#**interface port** *2*

Raisecom(config-port)# **clear oam event**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show oam event**

Raisecom#**show oam peer event**

24.4.9 Monitoring and maintenance

Command	Description
show oam	show OAM link local configuration and status
show oam peer	show OAM link information on opposite device
show oam loopback	show remote loop-back information
show oam event	show local device happening events
show oam peer event	show opposite device informing events
show oam notify	show all OAM link local events informing configuration
show oam statistics	show all OAM port link statistics information

24.4.10 Configuration example

According to Figure 1-1, if response remote loop-back, device A can be configured as below:

Raisecom#**config**

Raisecom(config)#**oam passive**

Raisecom (config)#**interface client** *1*

Raisecom(config-port)#**oam** *enable*

Raisecom (config-port)# **oam loopback process**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show oam loopback**

  Port: client1

  Loopback status: No

  Loopback react: Process

Chapter 26   Extended OAM

25.1 Extended OAM principle overview

Extended OAM, using IEEE802.3ah OAM to manage and monitor the remote device. It is composed by 3 parts:

1. Get the attribute of remote device;

2. Upload and down file of remote device;

3. Manage extended OAM link state and statistic.

Extended OAM includes the followings:

➢ Get remote attribute: the extended OAM attribute can be used to get the remote attribute form the center site.

➢ Set remote device: config the remote device, including host name, enable and disable port, duplex, bandwidth, fault transfer etc.

➢ Set remote device nettwork management parameter: can config remote device network management parameter, such as ip address, gateway, community parameter and management VLAN etc, then implement full management with SNMP protocol.

➢ Remote TRAP: when the port of remote device show LINK UP/DOWN, the remote device will send extended OAM notification fram to inform the center site, then the center device will send TRAP.

➢ Extended remote loopback: the remote optical port can be set loopback function, the function of whether to count repeatedly can be set.

➢ Reset remote device: send command to reset remote device.

➢ Other remote device function management: with the increasing of remote device, center device can manage more remote device with extended OAM function such as: SFP、Q-in-Q、Virtual Circuit diagnosis etc.

➢ Download remote file: the remote can get remote file from FTP/TFTP server. The file also can be send from the server to center device, then the remote device can get from the center device.

➢ Upload remote file: put the file to FTP/TFTP server, or from the remote device to center one, then put to server from the center device.

➢ Link statistic and management of extended OAM function.

Note: extended OAM link can only be established between center and remote site. The devices of two end must be set to master and passive, or the link can't be up.

25.2 Extended OAM management

25.2.1 Default extended OAM configuration

Function	Default configuration
Powered configuration request	Enable
Extended OAM notice	Enable
Remote end trap switch	open

25.2.2 Extended OAM configuration mode

To configure remote equipments on a local end equipment, you need to enter remote configuration mode. The steps to enter remote configuration mode are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *portid*: physical port ID
3	**remote-device**	Enter remote configuration mode

To configure remote equipment ports on local equipment, you need to enter remote interface configuration mode. The steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**interface client** *client-id*	Enter remote physical port configuration mode *Clinet-id* port ID

25.2.3 Remote equipment system configuration

Configure remote equipment system configuration, including configuring remote equipments' hostname, the maximum frame length, save and delete the configuration files.

The steps to configure remote equipment hostname and remote equipment maximum frame length are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**hostname** *HOSTNAME*	Configure remote equipment hostname *HOSTNAME* remote system network name
5	**system mtu** *<1500-8000>*	Configure remote equipment maximum frame length
6	**show remote-device information**	Show current remote equipment hostname and actual effective maximum frame length

Note: configure the maximum frame length of remote equipment; the actual effective value may be

different because of different remote equipment. For example, RC552-GE can configure remote maximum frame length to 1916 bytes or 1536 bytes. If the remote end is RC552-GE, and the configuration value is less than 1916, the effective value is 1536, or it is 1916.

The steps to save remote equipment configuration file is as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port**	**line**	**client**} *portid*	Enter ethernet physical port mode *portid*: physical port number
3	**remote-device**	Enter remote configuration mode
4	**write**	Save remote equipment configuration file

The steps to delete remote equipment configuration file is as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port**	**line**	**client**} *portid*	Enter ethernet physical port mode *portid*: physical port number
3	**remote-device**	Enter remote configuration mode
4	**erase**	Delete remote equipment configuration file

When executing the command to delete remote equipment configuration file, you need to confirm your operation.

Note:

➢ The operation to the configuration file is to save and delete the file on remote equipment, not to operate the local equipments file system.
➢ It takes a long time save and delete remote files, so when executing the command, there may be some unusual situations like OAM link breaking down.

25.2.4 Configure extended OAM protocol

The steps to enable/disable powered configuration request configuration are as follows:

Step	Command	Description
1	**config**	Enter global configuration
2	**extended-oam config-request** *enable* **extended-oam**	Enable/disable powered configuration request *enable*: enable powered configuration request

	config-request *disable*	*disable*: disable powered configuration request
3	**exit**	Return to privileged EXEC mode
4	**show extended-oam status**	Show extended OAM link state

The steps to disable/enable sending extended OAM notices configuration are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**extended-oam notification** *enable*	Enable/disable sending extended OAM notice
	extended-oam notification *disable*	*enable*: enable sending extended OAM notice *disable*: disable sending extended OAM notice
3	**exit**	Return to privileged EXEC mode
4	**show extended-oam notification**	Show OAM informing frame enable configuration state

25.2.5 Configure remote equipment port

➢   Configure remote equipment port enable/disable

The steps to disable remote equipment ports are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *portid*: port physical ID
3	**remote-device**	Enter remote configuration mode
4	**interface client** *client-id*	Enter remote physical port configuration mode *client-id:*port ID
5	**shutdown**	Shutdown remote equipment port

In remote port configuration mode, use **no shutdown** to enable remote equipment port.

➢   Configure remote equipment port rate/duplex

The steps to configure remote equipment ports rate/duplex are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode

3	**remote-device**	Enter remote configuration mode
4	**interface client** *client-id*	Enter remote physical port configuration mode
5	**speed** *{auto* / *10*/ *100* /*1000 }* **duplex** *{ full* / *half }*	Configure port rate and duplex mode

When the equipment has 1000M optical port, we can configure optical port auto-negotiation function, the steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**line-speed auto**	Configure remote equipment optical port auto-negotiation

In remote configuration mode, use **no line-speed auto** to shutdown optical port auto-negotiation function.

Note: when remote equipment is configured port rate/duplex, there may be some unusual situations like OAM link breaking down.

> ➢ Configure remote equipment port stream control/speed control

The steps to enable/disable remote equipment stream control are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *Portid* physcial port ID
3	**remote-device**	Enter remote configuration mode
4	**interface client** *client-id*	Enter remote physical port configuration mode
5	**flowcontrol** *{on/off}*	Enable/disable remote equipment port stream control function

The steps to configure remote equipment port in/out direction bandwidth are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port|line|client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID

Step	Command	Description
3	**remote-device**	Enter remote configuration mode
4	**rate-limit line** *line-id* **ingress** *rate* **rate-limit client** *client-id* **ingress** *rate*	Configure remote equipment port in direction bandwidth *Line-id* line port ID *Client-id* client port ID *Rate* bandwidth
5	**rate-limit line** *line-id* **egress** *rate* **rate-limit client** *client-id* **ingress** *rate*	Configure remote equipment port out direction bandwidth

Run **no rate-limit line** *line-id* **ingress** or **no rate-limit client** *client-id* **ingress** to restore in remote configuration mode.

Run **no rate-limit line** *line-id* **engress** or **no rate-limit client** *client-id* **egress** to restore in remote configuration mode.

➢ Configure remote equipment port description

The steps to configure remote port information are as follows:

Step	Command	Description
1	**config**	Enter global configuration
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**description line** *line-id WORD* **description client** *client-id WORD*	Configure remote equipment port description information *Line-id WORD* remote port description information *Client-id WORD* remote port description information

In remote configuration mode, use **no description line** *line-id* or **description client** *client-id WORD* to delete the description information.

In remote configuration mode, use **show interface port** and **show interface port detail** to show remote port configuration information.

➢ Start/shutdown extended remote loopback

Starting loopback function may affect data transmission.

Enable remote equipment optical port inside-loopback, you can select the parameter so that the response end could recalculate CRC. The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration ode

	2	interface {**port**|**line**|**client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
	3	**remote-device**	Enter remote configuration mode
	4	**inside-loopback** [**crc-recalculate**]	Start remote equipment optical port inside-loopback

In remote configuration mode, use **no inside-loopback** to stop remote equipment inside-loopback, use **show inside-loopback** to show remote optical port inside-loopback state and parameter.

➢ Run remote equipment line diagnoses function

Executing remote equipment line diagnoses function may affect the link and data transmission. The steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	interface {**port**|**line**|**client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**test cable-diagnostics**	Run remote equipment line diagnoses

In remote configuration mode, use **show cable-diagnostics** to show remote equipment line diagnoses result.

25.2.6 Upload/download files from remote equipment

➢ Download the file from server to remote equipment

The system bootroom file, startup file, startup configration file and FPGA file of remote device can be downloaded from server to remote device (center device as the relay). This function can be started by center device or remote device, and multiple remote devices can be upgraded at the same time.

Center device starts, download from FTP/TFTP server:

Step	Command	Description
1	**config**	Enter global configuration mode
2	interface {**port**|**line**|**client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**download** {**bootstrap** | **system-boot** | **startup-config** | **fpga**} **ftp** *A.B.C.D USRNAME PASSWORD FILENAME* **download** {**bootstrap** | **system-boot** | **startup-config** | **fpga**} **tftp** *A.B.C.D FILENAME*	Download the file from FTP server to remote equipment *A.B.C.D:* Server IP address *USRNAME:* FTP server username *PASSWORD:* FTP server password *FILENAME:* The filename on the server

		Download the files from TFTP server to remote equipment
		A.B.C.D: server IP address
		FILENAME: the filename on the server

Acting from the remote equipment, the steps to download files from FTP/TFTP server to remote end are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port**	**line**	**client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3		Download the file from FTP server to remote equipment
		A.B.C.D: Server IP address
	download {**bootstrap**|**system-boot**| **startup-config**	**fpga**} **ftp** *A.B.C.D USRNAME PASSWORD FILENAME* **download** {**bootstrap**|**system-boot**| **startup-config**	**fpga**} **tftp** *A.B.C.D FILENAME*	*USRNAME:* FTP server username
		PASSWORD: FTP server password
		FILENAME: The filename on the server
		Download the files from TFTP server to remote equipment
		A.B.C.D: server IP address
		FILENAME: the filename on the server

When the file downloading is over, the remote equipment can be shown with **dir** in privileged EXEC mode, and use **erase** to delete.

➢ Upload files to the server from remote equipment

The system bootroom file and startup configuration file on the remote equipment can be transmitted through local end to do uploading from remote equipment to the server. The function can be started by local equipment or remote equipment. When it is started from local equipment, we can no upgrade several remote equipments at the same time.

Started from local equipment, the steps to upload file from remote equipment to FTP/TFTP server are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port**	**line**	**client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**upload** {**startup-config**	**system-boot** } **ftp** *A.B.C.D*	Upload file from remote equipment to FTP server *A.B.C.D:* Server IP address

	USRNAME PASSWORD FILENAME	USRNAME: FTP server username
		PASSWORD: FTP server password
	upload {**startup-config** |	FILENAME: The filename on the server
	system-boot} **tftp** A.B.C.D	Upload file from remote equipment to TFTP server
	FILENAME	A.B.C.D: server IP address
		FILENAME: the filename on the server

Started from remote equipment, the steps to upload file from remote equipment to FTP/TFTP server are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** portid	Enter ethernet physical interface mode
		Portid physical port ID
3		Upload file from remote equipment to FTP server
	upload {startup-config |	A.B.C.D: Server IP address
	system-boot } ftp A.B.C.D	USRNAME: FTP server username
	USRNAME PASSWORD FILENAME	PASSWORD: FTP server password
	upload {startup-config |	FILENAME: The filename on the server
	system-boot } tftp A.B.C.D	Upload file from remote equipment to TFTP server
	FILENAME	A.B.C.D: server IP address
		FILENAME: the filename on the server

> ➢ Download remote equipment file from the server to local end

The remote equipment system bootroom file, startup file, startup configuration file and FPGA file can all be downloaded from server to local end using FTP/TFTP protocol, then be saved in local FLASH file system with a designated filename, making preparation for further upgrading.

When local end saves remote file, it will add postfix automatically according to the file type, so the local filename designated by user does not need postfix. What's else, the filename designated by remote file can not be the same with the filename of local end its own in flash. That is, the remote equipment's bootroom file can not be named as system-boot; the remote equipment's startup configure file can not be named as startup-config; the remote equipment's FPGA file can not be named as FPGA. However, the system bootroom file is not saved in FLASH, so the bootroom file of remote equipment can be named as bootstrap.

In privileged EXEC mode, the steps to download remote equipment file from the server to local end are as follows:

Step	Command	Description
1	**download {remote-bootstrap |**	A.B.C.D: server IP address
	remote-system-boot |	USRNAME: FTP server username
		PASSWORD: FTP server password

	remote-startup-config|remote-fpga} ftp *A.B.C.D USRNAME PASSWORD FILENAME LOCAL-FILENAME* **download { remote-bootstrap | remote-system-boot | remote-startup-config|remote-fpga} tftp** *A.B.C.D FILENAME LOCAL-FILENAME*	*FILENAME:* the filename on FTP server *LOCAL-FILENAME:* the filename saved in local end *A.B.C.D:* server IP address *FILENAME:* the filename on the server *LOCAL-FILENAME:* the filename saved on local end

When the downloading is over, you can use **dir** to show the state in privileged EXEC mode on local equipments, and use **erase** to delete.

➢ Upload remote equipment file from local end to the server

The remote file saved in local equipment's FLASH can be uploaded using FTP/TFTP to the server. The steps are as follows:

Step	Command	Description
1	**upload {remote-bootstrap | remote-system-boot | remote-startup-config|remote-fpga} ftp** *A.B.C.D USRNAME PASSWORD FILENAME LOCAL-FILENAME* **upload {remote-bootstrap | remote-system-boot | remote-startup-config|remote-fpga} tftp** *A.B.C.D FILENAME LOCAL-FILENAME*	*A.B.C.D:* server IP address *USRNAME:* FTP server username *PASSWORD:* FTP server password *FILENAME:* the filename on FTP server *LOCAL-FILENAME:* the filename saved in local end *A.B.C.D:* server IP address *FILENAME:* the filename on the server *LOCAL-FILENAME:* the filename saved on local end

➢ Download file from local end to remote equipment

The remote file saved in local equipment FLASH, can be downloaded to remote equipment using extended OAM protocol. The function can be started from local equipment or remote equipment. When started from local equipment, several remote equipments can be upgraded at the same time.

Started from local equipment, the steps to download file from local end to remote equipments are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** *portid*	Enter Ethernet physical interface mode
3	**remote-device**	Enter remote configuration mode
4	**download { bootstrap | system-boot | fpga }** *FILENAME* **download startup-config**	Download bootroom file, startup file and FPGA file from local end to remote equipment

	[*FILENAME*]	*FILENAME:* the filename on local end
		Download configuration file from local end to remote equipment
		FILENAME: the filename on local end

Started from remote end, the steps to download file from local end to remote end are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port	line	client}** *portid*	Enter ethernet physical interface mode
		Portid physical port ID
3	**download {bootstrap	system-boot	fpga}** *FILENAME*	Download bootroom file, startup file and FPGA file from local end to remote equipment
		FILENAME: the filename on local end
	download startup-config [*FILENAME*]	Download configuration file from local end to remote equipment
		FILENAME: the filename on local end

When file download is over, you can use **dir** to show the state in privileged EXEC mode on remote equipment and use **erase** to delete.

25.2.7 Configure remote equipment to network management enabled equipment

➢ Configure remote equipment SNMP community and IP address

The steps to configure remote equipment community name and IP address are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port|line|client}** *portid*	Enter Ethernet physical interface mode
		Portid physical port ID
3	**remote-device**	Enter remote configuration mode
4	**snmp-server community** *community-name {ro|rw}*	Configure remote equipment community name and priority.
		community-name community name
		ro read only
		rw read & write
5	**ip address** *ip-address* [*ip-mask*] *vlan-list*	Configure remote equipment IP address
		ip-address
		ip-mask
		vlan-list: the managed VLAN list

In remote configuration mode, use **no snmp-server community** *community-name* to delete remote

equipment community name.

When configuring IP address we need to designate and manage VLAN as well, if the VLAN does not exist, create VLAN (by default all the ports are member port); if related VLAN exists, the member port configuration will not be modified. In remote configuration mode, use **no ip address ip-address** to delete remote port IP address.

In remote configuration mode, use **show remote-device information** to show remote community name and IP address information.

> Configure remote equipment Q-in-Q

Configure remote equipment flexible Q-in-Q function, the attributions that need to be configured include: switch mode, TPID, local VLAN and access interface.

When configuring remote equipment to complete transparent mode, the other configurations, like TPID, local VLAN and access interface, are all not available. The steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port	line	client}** *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**switch-mode transparent**	Configure remote equipment to complete transparent mode

When configuring remote equipment to Dot1q VLAN transparent mode, or single TAG mode, local VLAN and access port is valid, while TPID is not. When the equipment is configured to single TAG mode, the data packet coming from the access port will be marked local VLAN ID TAG if it has no TAG; if it has, it will not be handled.

The configuration steps are as follows;

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port	line	client}** *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**switch-mode dot1q-vlan native-vlan** *<1-4094>* **[line]**	Configure remote equipment to Dot1q VLAN transmission mode **native-vlan:** local VLAN *<1-4094>:* VLAN ID; **line**: Line port is the access port, when the keyword line is not selected, it means that client port is the access port

Configure remote equipment to Double tagged VLAN transmission mode, that is in double TAG mode, TPID, local VLAN and access port are all valid. When the equipment is configured double TAG mode, the data packet coming from the access port will be marked specific TPID and local VLAN ID outer layer TAG, whatever it has TAG or not.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port|line|client}** *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**switch-mode double-tagged-vlan [tpid** *HHHH***] native-vlan** *<1-4094>* **[line]**	Configure remote equipment to Double tagged VLAN transmission mode **native-vlan:** local VLAN; *<1-4094>:* VLAN ID; **Line:** Line port is the access port **tpid:** outer-layer tagged TPID *HHHH:* outer-layer tagged TPID, hexadecimal number, 0000 to FFFF When tpid is not configured, it means the TPID that takes 0x9100 as the outer-layer TAG

In remote configuration mode, run **show remote-device information** to show remote equipment flexible Q-in-Q function related configuration.

25.2.8 Save remote equipment configuration information to local end

When remote equipment belongs to RC552 serious, the equipment itself will not save configuration file, but it is able to save remote configuration content to local end using **writ local.** When the local equipment is rebooted, it will load the saved 552 configuration file, and if there is configuration request from remote 552, the saved configuration will be sent to remote end. The saving steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port|line| lient}** *portid*	Enter ethernet physical interface mode *Portid* physical port mode
3	**remote-device**	Enter remote configuration mode
4	**write local**	Save remote configuration to local FLASH

If there is no 552 configuration file when local end is started, and local end has not sent configuration to remote 552 yet after booting, execute the command and you will be failed.

Saving FLASH file takes a long time, so when executing the command, unusual situations like OAM link

breaking down may happen.

25.2.9 Reset remote equipment

The steps to reset remote equipment are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port|line|client}** *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**reboot**	Reset remote equipment

You need to confirm you operation after reset command is executed.

When remote equipment is resetting or rebooting, OAM link may break down, and local equipment may lose the connection to remote equipment.

25.2.10 Extended OAM statistic clear function

Extended OAM counts the sending and receiving extended OAM messages number on each OAM link, the extended OAM message types include: variable acquirement and response, variable setting and response, file request and file data, notice and so on. User can follow the steps below to clear statistic information:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**clear extended-oam statistics [port-list** *port-list*] **clear extended-oam statistics [line-list** *line-list*] **clear extended-oam statistics [client-list** *client-list*]	Clear extended OAM link static information

25.2.11 Monitoring and maintenance

Command	Description
show interface port	Show remote equipment port information
show interface port detail	Show remote equipment port detailed information
show interface port statistics	Show remote equipment port static information
show oam capability	Show remote equipment ability of supporting OAM management

|	
show remote-device information	Show remote equipment basic information
show sfp	Show remote equipment SFP information
show cable-diagnostics	Show link diagnoses result
show inside-loopback	Show remote loopback state and parameter
show extended-oam statistics	Show extended OAM frame static information
show extended-oam status	Show extended OAM link state
show snmp trap remote	Show remote trap enable configuration

25.2.12 Typical configuration example
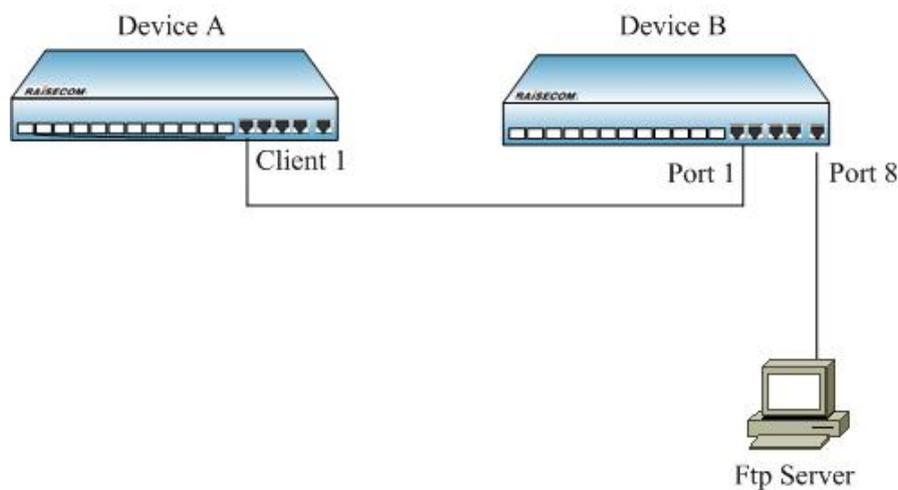
Fig 1 remote file upload/download function typical configuration

If you want to back-up and upgrade device A's startup configuration file on device B, configure B as the steps below:

1) upload startup configuration file to the server from remote device

Raisecom#**config**

Raisecom(config)# **interface port** *1*

Raisecom (config-port)# **remote-device**

Raisecom(config-remote)# **upload startup-config ftp** *12.0.0.1 raisecom raisecom configfile_version_1*

2) download startup configuration file to remote device from the server:

Chapter 27   Loopback Detection

26.1 Loopback detection introduction

Loopback detection is to solve the network problem due to Loop (inner loop and outer loop), so as to enhance the network self-diagnostic capability, fault compatibility and robustness.
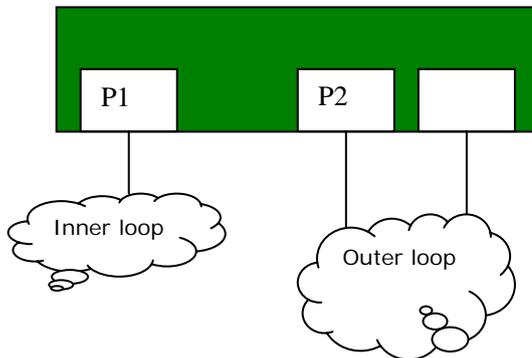

Fig 1

The loop discovery process:

> ➤ Each port of the switch sends Loopback-detection packet periodically (the interval is configurable, generally as 4 seconds)
> ➤ Switch will check the CUP MAC section of received packet, if the CPU MAC section has the same MAC as the switch, loop exsits on certain ports; otherwise, packet will be dropped;
> ➤ If the port series number which sends out packed is the same with the port number which receives packets, self loopback exists; otherwise, outer loop exists;
> ➤ When loop exists, port with bigger series number will be shutdown;

Notice: When several loops exists, all the ports may be shutdown.

26.2   Default port loopback detection configuration

Command	Default value
Enable/disable loopback detection function	Enable all the ports loopback detection function
Configure the type of loopback detection function and destination address type	Destination MAC will be the broadcasting address
Configure the operation time of port's receiving/sending packet shutdown	The loop can not recover when it is shutdown
Configure the loopback detection time hello time	The hello time time of loopback detection is 4s.

26.3   Configure loopback detection function

Loopback detection function configuration includes the four parts follow:

- ➢ Enable/disable loopback detection function
- ➢ Configure loopback detection type, or destination address type
- ➢ Configure the operation time of loop port receiving/sending packet shutdown
- ➢ Configure loopback detection hello time

To enable/disable loopback detection function:

Step	Command	Description
1	**config**	Enter global configuration function
2	**loopback-detection** {*enable | disable*} **port-list** {*port-list|all*}	Enable/disable the given port's loopback function. By default it is enabled *Enable*, enable loopback detection function *Disable*, disable loopback detection function *port-list* physical port number, use ',' and '_' for multi-ports input *All* all the ports
3	**exit**	Quit from global configuration mode and enter privileged EXEC mode
4	**show loopback-detection**	Show port loopback detection state

To configure loopback detection type (destination address type)

Step	Command	Description
1	**config**	Enter global configuration mode
2	**loopback-detection destination-address** [*mac-address* **vlan** *vlan-id*]	Configure loopback detection type or destination address type, including unicast packet, multicast packet and broadcast packet. Configure multicast and unicast as pointing to the stable MAC of CPU port and writing into hardware address table. By default it is sending broadcast packet
3	**exit**	Quit from global configuration mode and enter privileged EXEC mode
4	**show loopback-detection**	Show port loopbcak detection state

Configure the operation time of shutting down the receiving/sending packet of the loop port:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** *portnumber*	Enter physical port configuration mode
3	**loopback-detection down-time** *{<0-65534>|infinite}*	The operation time of shutting down the receiving/sending packet of the loop port when a loop is detected <0-65534> the time that the loop port is in down state Infinite: the loop port can not recover when disabled
4	**exit**	Quit from physical port mode and enter global configuration mode

| 5 | **exit** | Quit from global configuration mode and enter privileged EXEC mode |
| 6 | **show loopback-detection** | Show the port loopback detection state |

To configure loopback detection hello-time

Step	Command	Description
1	**config**	Enter global configuration mode
2	**loopback-detection hello-time** *<1-65535>*	Configure loopback detection hello-time. 1-65535, the interval of sending detection packet, unit is second, by default it is 4s;
3	**exit**	Quit from global configuration mode and enter privileged EXEC mode
4	**show loopback-detection**	Show port loopback detection state

To restore default configuration use global configuration command: no loopback-detection hello-time.

26.4   Monitoring and maintenance

Show port loopback detection state:

Show loopback-detection

Show loopback detection hello-time, destination address. Showing loopback detection state includes loopback detection function switch states: enable, disable; if there is port loopback: yes, no; port state/shutdown time; the source port that is in the loop with this port.

26.5   Typical configuration example

The topology structure is shown below:
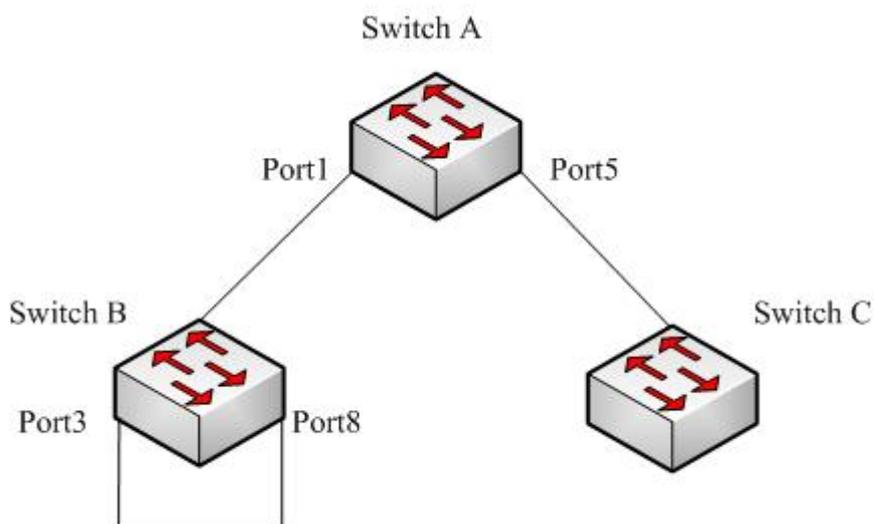
Fig 2 Loopback detection topology structure

As is shown in figure 1, configure Switch2 and Switch3 to loopback detection disable, and configure

Switch1 to loopback detection enabled, when there is loop between Port3 and Port8 of Switch, Switch will detect loop and shut the Port1 of Switch1.

Switch1configuration is shown below:

Raisecom# **config**

Raisecom(config)# **loopback-detection hello-time** *3*

Raisecom(config)# **loopback-detection** enable **port-list** *all*

Raisecom(config)# **exit**

Raisecom# **show loopback-detection**

Period of loopback-detection: 3 s

VLAN: 1

Destination address: FFFF.FFFF.FFFF

Port   Detection State   Loop Flag   State/Time   Source Port

---

Port	*Detection State*	*Loop Flag*	*State/Time*	*Source Port*
1	*enable*	*yes*	*down/infin*	*1*
2	*enable*	*no*	*--/infin*	*--*
3	*enable*	*no*	*--/infin*	*--*
4	*enable*	*no*	*--/infin*	*--*
5	*enable*	*no*	*--/infin*	*--*
6	*enable*	*no*	*--/infin*	*--*
7	*enable*	*no*	*--/infin*	*--*
8	*enable*	*no*	*--/infin*	*--*
9	*enable*	*no*	*--/infin*	*--*
10	*enable*	*no*	*--/infin*	*--*
11	*enable*	*no*	*--/infin*	*--*
12	*enable*	*no*	*--/infin*	*--*
13	*enable*	*no*	*--/infin*	*--*
14	*enable*	*no*	*--/infin*	*--*
15	*enable*	*no*	*--/infin*	*--*
16	*enable*	*no*	*--/infin*	*--*
17	*enable*	*no*	*--/infin*	*--*
18	*enable*	*no*	*--/infin*	*--*
19	*enable*	*no*	*--/infin*	*--*
20	*enable*	*no*	*--/infin*	*--*
21	*enable*	*no*	*--/infin*	*--*
22	*enable*	*no*	*--/infin*	*--*
23	*enable*	*no*	*--/infin*	*--*
24	*enable*	*no*	*--/infin*	*--*

Switch2 configuration is shown below:

Raisecom# **config**

Raisecom(config)# **loopback-detection** disable **port-list** *all*

Raisecom(config)# **exit**

Raisecom# **show loopback-detection**

Period of loopback-detection: 4 s

VLAN: 1

Destination address: FFFF.FFFF.FFFF

Port	Detection State	Loop Flag	State/Time	Source Port
1	*disable*	*no*	*--/infin*	*--*
2	*disable*	*no*	*--/infin*	*--*
3	*disable*	*no*	*--/infin*	*--*
4	*disable*	*no*	*--/infin*	*--*
5	*disable*	*no*	*--/infin*	*--*
6	*disable*	*no*	*--/infin*	*--*
7	*disable*	*no*	*--/infin*	*--*
8	*disable*	*no*	*--/infin*	*--*
9	*disable*	*no*	*--/infin*	*--*

Switch3 configuration is shown below:

Raisecom# **config**
Raisecom(config)# **loopback-detection** *disable* **port-list** *all*

Raisecom(config)# **exit**

Raisecom# **show loopback-detection**

Period of loopback-detection: 4 s

VLAN: 1

Destination address: FFFF.FFFF.FFFF

Port	Detection State	Loop Flag	State/Time	Source Port
1	*disable*	*no*	*--/infin*	*--*
2	*disable*	*no*	*--/infin*	*--*
3	*disable*	*no*	*--/infin*	*--*
4	*disable*	*no*	*--/infin*	*--*
5	*disable*	*no*	*--/infin*	*--*
6	*disable*	*no*	*--/infin*	*--*
7	*disable*	*no*	*--/infin*	*--*
8	*disable*	*no*	*--/infin*	*--*

9   disable   no   --/infin   --

Chapter 28   DHCP

27.1 System Overview

This chapter is mainly about how to configure and maintain DHCP snooping on switches, which includes:

- ✧ DHCP Snooping principle
- ✧ DHCP Snooping configuration
- ✧ Monitoring and maintenance
- ✧ DHCP Snooping trouble shooting

27.1.1 DHCP Snooping principle

Introduction:

If there is private DHCP server in the network, user may get wrong IP address. DHCP Snooping is a safe feature of DHCP, it provides network safety by filtrating the unbelievable DHCP message and establishing and maintaining a DHCP Snooping binding database (or DHCP Snooping binding table). To let user get IP address from valid DHCP server, DHCP Snooping safety mechanism allows the port to be set to creditable port and unauthentic port. It divides creditable port from unauthentic port on the switch, filtrates the unauthentic DHCP response message to insure the network safety. It is like firewall between unauthentic host and DHCP server.

Unauthentic DHCP message is the message that the host received from the network or outside the firewall. When DHCP Snooping is used in the network that provides network services, unauthentic message is from other network which does not belong to the server network, like user switch. The messages that are from unknown equipments may be attacking source, so it is unauthentic. At the same time, to make sure the network safety, network administrator may need to record the user's IP address when user is online, to make sure the correspondence relationship between the IP address that user gets from DHCP server and user host MAC address. By monitoring DHCP Request and DHCP ACK broadcast message received by the creditable port, DHCP Snooping records the client MAC address and the IP address acquired to actualize the function.

In the network that provides services, the creditable port is connected with DHCP server; the unauthentic port is connected with client side, or with other equipments in the network. The unauthentic port will drop the DHCP-ACK, DHCP-NAK and DHCP-OFFER message that is received from DHCP response (because these equipments that are connected with unauthentic ports should not make any response to DHCP server); while the response message received b the creditable port will be transmitted normally, which will prevent pseudo-server deception and make sure that user can get the correct IP address.

Fig 1-1 is a typical network picture of DHCP Snooping:
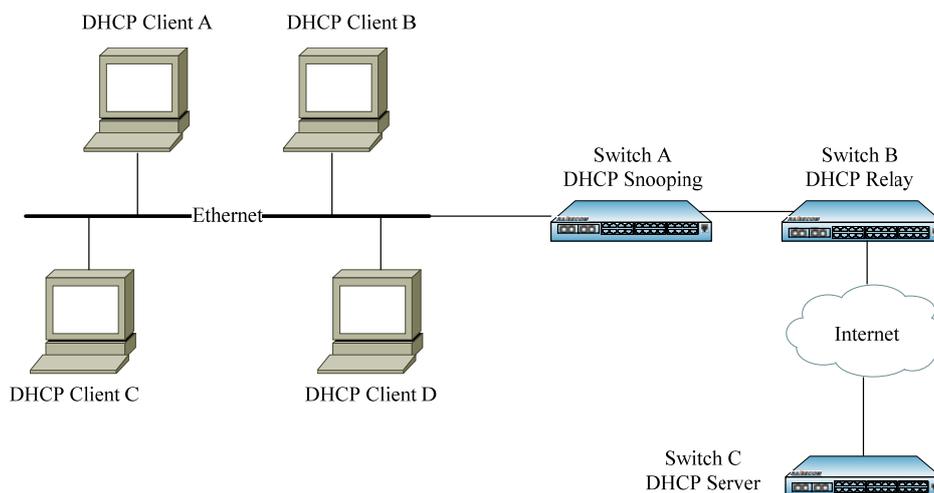
Fig 1-1 DHCP Snooping typical network structure

Option 82 overview:

Option 82 is the Relay Agent Information option of DHCP message, which is identified in request document RFC3046. When DHCP Client sent request message to DHCP Server, if it is needed to cross DHCP Snooping, DHCP Snooping will add Option 82 to request message. Option 82 contains much sub-option. The option 82 introduced here support sub-option 1 and sub-option 2:

sub-option 1: circuit ID is defined in it

sub-option 2: remote ID is defined in it

sub-option 1: sub-option 1 is a sub-option of Option 82, which is circuit ID sub-option. A sub-option is usually configured on DHCP Snooping equipment or repeaters, which defines the port number of the switch port that needs to carry DHCP client when transmitting messages and the port's VLAN number. Usually sub-option1 and sub-option 2 need to be used together to note the information of DHCP source port.

Sub-option 2: it is also a sub-option of Option 82, which is Remote ID. This sub-option is usually also configured on DHCP repeater, which defines the MAC address information of the equipments that carry Snooping or repeater equipment. Usually sub-option 1 needs to be used together to note DHCP source port information.

Option 82 actualize the address information of DHCP client and DHCP snooping equipment or repeater equipment's record on DHCP server, with the help of other software it could actualize DHCP distribution restriction and billing function. For example, combined with IP Source Guard, the reception of IP address + MAC address can be defended effectively.

Option 82 handling actions:

- ➢ When the switch receives a request message without Option 82 words, if it supports Option 82, Option 82 will be added and transmitted.
- ➢ When the switch receives a request message without Option 82 words, if it supports Option 82, Option 82 will be transmitted; if not, the message will be dropped.
- ➢ When the switch receives a request message without Option 82 words, if it supports Option 82, Option 82 will be deleted and transmitted; if not, the message will be dropped.

The structure of Option 82 message:

Option 82 obeys 'TLV' option format, fig 1-2 shows its message structure:

1	1	1	1	4	1	1	6
82	14	1	4	VLAN(2)+MODULE(1)+PORT(1)	2	6	MAC ADDRESS(6)

option 82   Sub option 1 (Circuite ID)   Sub option 2 (Remote ID)
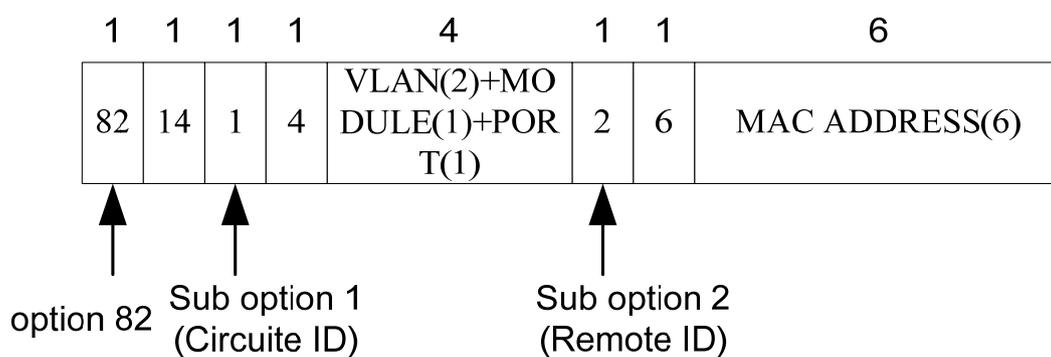
Fig 1-2 Option 82 message structure

27.1.2 Configure DHCP Snooping

The part describes how to configure DHCP Snooping on the switch, including:

- ✧ Default DHCP Snooping configuration
- ✧ DHCP Snooping configuration guide
- ✧ Global DHCP Snooping configuration
- ✧ Port trust configuration
- ✧ DHCP Snooping supporting Option 82 configuration

27.1.2.1 Default DHCP Snooping configuration

Function	Default value
Global DHCP Snooping state	Disabled
Port DHCP Snooping state	Enabled
Port trust state	Untrusted
DHCP Snooping supporting Option 82	Disabled

27.1.2.2 DHCP Snooping configuration guide

- ➢ Make sure that the switch DHCP Server or DHCP Relay is not enabled;
- ➢ Global DHCP Snooping must be enabled;
- ➢ If DHCP Snooping is not enabled on the port, DHCP Snooping can not is not available on the switch;
- ➢ After DHCP Snooping is on, DHCP Server or DHCP Relay can not be started on the switch;
- ➢ If only DHCP Snooping is enabled, while DHCP Snooping supporting Option 82 is not, the switch will not insert Option 82 in the message nor handle the message that contains Option 82;
- ➢ Make sure the port that connects DHCP server is credible, while the port that connects client side is incredible.

27.1.2.3 Configure global DHCP Snooping

By default, global DHCP Snooping is off. Only when global DHCP Snooping is enabled can the switch DHCP Snooping take effect. To enable global DHCP Snooping, take the following steps:

The configuration step is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp snooping**	Enable global DHCP Snooping
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp snooping**	Show DHCP Snooping configuration

Note: If the switch enables DHCP Server or DHCP Relay, global DHCP Snooping can not be started. On the opposite, if the switch enables DHCP Snooping, DHCP Server or DHCP Relay can not be started.

Use global configuration command **no ip dhcp snooping** to disable global DHCP Snooping.

27.1.2.4 Configure port DHCP Snooping

By default, DHCP Snooping is on, use **no ip dhcp snooping port-list** to close port DHCP Snooping.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp snooping port-list** *4-9*	Enable DHCP Snooping on port 4-9
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp snooping**	Show DHCP Snooping configuration

Notice: By default, all the ports' DHCP Snooping of the switch is on. But until global DHCP Snooping is on can they be available. That is to say, if global DHCP Snooping is off, and only port DHCP Snooping is on, DCHP Snooping can not take effect.

27.1.2.5 Configure port trust

Unauthentic port will drop DHCP-ACK, DHCP-NAK, DHCP-OFFER message received from DHCP server response (because these equipments connected by unauthentic ports should not make any DHCP server response). While the DHCP server response message received by credible port will be transmitted normally.

Credible port connects DHCP server or the ports of others switches, while unauthentic port connects user or network, which keeps away from server deception, and makes sure user can get the correct IP address.

Follow the steps below to set the designated port to credit port.

Step	Command	description
1	**config**	Enter global configuration mode
2	**interface port 15**	Enter port configuration mode
3	**ip dhcp snooping trust**	Configure credit port
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode

| 6 | **show ip dhcp snooping** | Show DHCP Snooping configuration |

Notice: Only when port trust is started in global DHCP Snooping and the port has also started DHCP Snooping can it take effect. Use **no ip dhcp snooping turst** to set the port to unauthentic port.

In port configuration mode use **no ip dhcp snooping trust** to set the port to unauthentic port and delete it from trust port list.

27.1.2.6 Configure DHCP Snooping supporting Option 82

Following the steps below, user can enable DHCP Snooping supporting Option 82, and the switch will add Option 82 option into the DHCP request message that receives Option 82; delete Option 82 in the DHCP response message that contains Option 82. The received DHCP request message that contains Option 82 will be handled according to the configured strategy and transmitted, while to the response message that don't contain Option 82 option, the switch will not take any action and transmit it directly.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp snooping information option**	Enable DHCP Snooping supporting Option 82
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp snooping**	Show DHCP Snooping configuration

Notice: DHCP Snooping supporting Option 82 function is global, but it reacts on the port. It can be enable only in global DHCP Snooping, and only when the port start DHCP Snooping can Option 82 take effect on the port.

Use global configuration command **no ip dhcp snooping information option** to stop DHCP Snooping supporting Option 82.

27.1.3 Monitoring and maintaining

Use the command **show** to look over the switch DHCP Snooping running state and configuration state and help monitoring and maintaining.

Command	Description
show ip dhcp snooping	Show DHCP Snooping configuration

Use **show ip dhcp snooping** to show DHCP Snooping configuration information, including global DHCP Snooping state, if Option 82 is supported, port DHCP Snooping state and port trust. Specific steps are as follows:

Raisecom#**show ip dhcp snooping**

DHCP Snooping: Enabled

Option 82: Enabled

Port   Enabled Status   Trusted

1	*enabled*	*no*
2	*enabled*	*no*
3	*enabled*	*no*
4	*enabled*	*no*
5	*enabled*	*no*
6	*enabled*	*no*
7	*enabled*	*no*
8	*enabled*	*no*
9	*enabled*	*no*
10	*enabled*	*no*
11	*enabled*	*no*
12	*enabled*	*no*
13	*enabled*	*no*
14	*enabled*	*no*
15	*enabled*	*yes*
16	*enabled*	*no*
17	*enabled*	*no*
18	*enabled*	*no*
19	*enabled*	*no*
20	*enabled*	*no*
21	*enabled*	*no*
22	*enabled*	*no*
23	*enabled*	*no*
24	*enabled*	*no*
25	*enabled*	*no*
26	*enabled*	*no*

27.1.4 Typical configuration example

This part gives a introduction to a example that a DHCP client connects DHCP server and get IP address dynamically through DHCP Snooping, it show the typical configuration of DHCP Snooping.

1. Configuration explanation:

This example is a simple and typical DHCP configuration, the two DHCP clients use DHCP port 2, 3 respectively to connect DHCP server.

- ➢ Configure the correct address pool on DHCP Server, and enable DHCP Server function globally.
- ➢ Enable DHCP Snooping function globally on DHCP Snooping equipment, and enable DHCP Snooping on the port, set port 1 to credible port, and configure DHCP Snooping supporting Option 82, use the default strategy Replace to handle the request messages from client side.

2. Topology picture
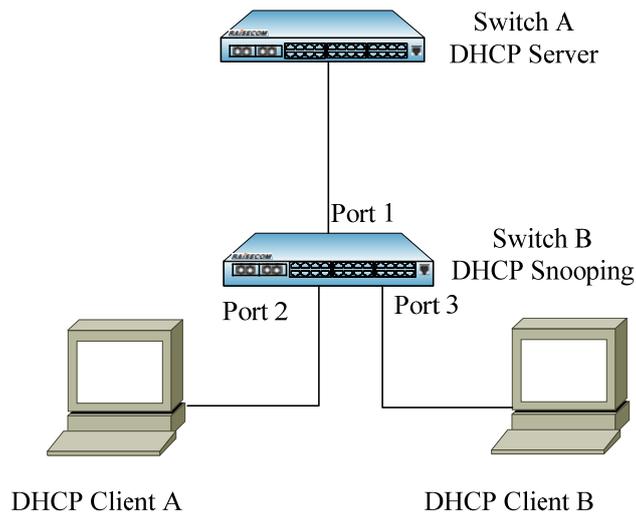
Fig 1-3 Typical DHCP Snooping configuration topology

3. Configuration step

   Configure DHCP Snooping:

   ➢ Enable global DHCP Snooping:

   Raisecom#**config**

   Raisecom(config)#**ip dhcp snooping**

   ➢ Port enable DHCP Snooping:

   Raisecom(config)# **ip dhcp snooping port-list** *1-3*

   ➢ Set port 3 to DHCP Snooping credible port:

   Raisecom(config)# **interface port 1**

   Raisecom(config_port)# **ip dhcp snooping trust**

   ➢ Enable DHCP Snooping supporting Option 82:

   Raisecom(config)#**ip dhcp snooping information optio**n

4. Show the result

On ISCOM switch use command **show ip dhcp snooping** to look over the switch DHCP Snooping running state and configuration state, on the client side use **show ip dhcp client** to show client IP address application. Specific contents are as follows:

Raisecom#**show ip dhcp snooping**

  DHCP Snooping: Enabled

  Option 82: Enabled

  Port   Enabled Status   Trusted

  ---

 1   enabled   yes

 2   enabled   no

   3   enabled   no

   ...   .

Raisecom#**show ip dhcp client**

Hostname:	*raisecomFTTH*
Class-ID:	*raisecomFTTH-3.6.1025*
Client-ID:	*raisecomFTTH-000e5e8a0798-IF0*
Assigned IP Addr:	*10.0.0.5*
Subnet mask:	*255.0.0.0*
Default Gateway:	*10.0.0.1*
Client lease Starts:	*Jan-01-2007 08:00:41*
Client lease Ends:	*Jan-11-2007 11:00:41*
Client lease duration:	*874800(sec)*
DHCP Server:	*10.100.0.1*
Tftp server name:	*--*
Tftp server IP Addr:	*10.168.0.205*
Startup_config filename: 2109.conf	

27.1.5 DHCP snooping trouble shooting

If DHCP client can not get network address normally through DHCP Snooping, it may be one of the following situations:

➢ If global DHCP Snooping and port DHCP Snooping are enabled at the same time;
➢ If DHCP Snooping do not open Option 82 option, when DHCP Snooping receives the message that contains Option 82 it will be dropped directly;
➢ If DHCP Snooping Option 82 option is enabled, and the request message handling strategy is set to be DROP, then the messages that contain Option 82 will be dropped;
➢ If the port is not configured as DHCP Snooping credible port, all the response messages to the ports mentioned above will be dropped.

If the configuration above still can not help, please examine if the equipment that opened DHCP Snooping has opened router function, examine if the DHCP server address is correct.

27.2 DHCP Server Configuration

This chapter is mainly about how to configure and maintain DHCP Server on the switch, including:

✧ DHCP Server principle overview
✧ DHCP Server configuration
✧ Monitoring and maintaining
✧ Typical configuration example
✧ DHCP Server trouble shooting

27.2.1 DHCP Server principle overview

Dynamic Host Configuration Protocol (DHCP) let the client acquire configuration information protocol in

TCP/IP network, which is based on BOOTP protocol, and adds the function of automatic distribution useful network address and so on based on BOOTP protocol. The two protocol can make interoperability through some mechanism. DHCP offers the network hosts configuration parameters, which are made of two parts: one is to transmit special configuration information to network hosts, the other one is to assign network addresses to the hosts. DHCP is based on client/server mode, in this mode specific host assigns network addresses and transmits network configuration parameters to network hosts, the designated hosts are called server.

Usually, in the following situations DHCP server will be used to accomplish IP address distribution:

(1) When the network scope is too large for manual configuration or centralized management to the whole network.

(2) When the network host number is larger than the IP address number that the network supports, and can not give each host a stable IP address; there is also user number limit who can get into the network at the same time (for example, Internet access service provider belongs to the situation), lots of users have to acquire their own IP address dynamically from DHCP server.

(3) When there is not so many hosts who need stable IP address, and most hosts have no the need for stable IP address.

In typical DHCP application, there is usually one DHCP server and several client (like PC and portable machine), the typical DHCP application is shown below:
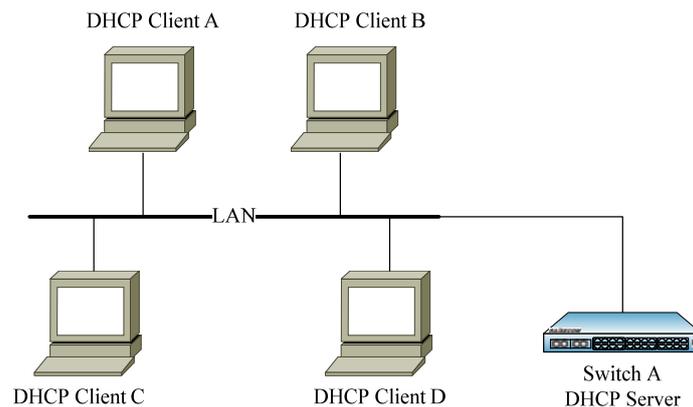
Fig 2-1 DHCP typical usage

27.2.2 Configure DHCP Server

This part is mainly about how to configure DHCP Server on the switch, including:

- ✧ Default DHCP Server configuration
- ✧ DHCP Server configuration guide
- ✧ Global DHCP Server configuration
- ✧ IP interface DHCP Server configuration
- ✧ Address pool configuration
- ✧ Lease table timeout configuration
- ✧ Border upon surrogate IP address configuration

Notice: Only ISCOM3000 serial switches support border upon surrogate IP address configuration.

27.2.2.1 Default DHCP Server configuration

Function	Default value
Global DHCP Server state	Disabled
IP port DHCP Server state	Disabled
Address pool	N/A
Lease table timeout	Maximum timeout: 1080 minutes Least timeout: 30 minutes Default timeout: 30 minutes
Neighbour proxy address	N/A

27.2.2.2 DHCP Server configuration guide

1. Make sure that DHCP Snooping on the switch is not on;

2. Global DHCP Server must be enabled;

3. If DHCP Server is not enable in IP port, DHCP Server does not take effect on this IP port;

4. When DHCP Server is on, DHCP Snooping can not be started either on the switch;

5. Make sure that the connection to DHCP Relay and DHCP server is correct, and the IP port address and the corresponding address pool range is correct.

6. If the client connect DHCP server through DHCP Relay, DHCP server must be ISCOM3000 serial switches. Except making sure IP port address and address pool configuration correct, correct configuration to neighbour proxy address and DHCP Relay.

27.2.2.3 Configure global DHCP Server

By default, global DHCP Server is disabled. Only when global DHCP Server is enabled, the switch DHCP Server can take effect. User can follow the steps below to start global DHCP Server:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp server	Enable global DHCP Server
3	exit	Return to privileged EXEC mode
4	show ip dhcp server	Show DHCP Server configuration

Notice: If DHCP Snooping has been started on a switch, global DHCP Server can not be started any more. On the opposite, if global DHCP Server has been started, DHCP Snooping can not be started.

Use global configuration command **no ip dhcp server** to close global DHCP Server.

27.2.2.4 Configure IP port DHCP Server

By default, IP port DHCP Server function is disabled as well, user can use IP port command **ip dhcp server** to start IP port DHCP Server function. To close IP port DHCP Server, use IP port command **no ip dhcp server.**

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip 4**	Enter IP port 4 configuration mode
3	**ip dhcp server**	Enable DHCP Server
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp server**	Show DHCP Server configuration

Notice: When global DHCP Server is off, user can start DHCP Server beforehand on a certain IP interface, but only when global DHCP Server starts, can the DHCP Server started from the IP port take effect.

27.2.2.5 Configure address pool

DHCP server selects and distributes IP address and other parameters from the address pool for the client. When the equipment that is selected as DHCP server receives a DHCP request from the client, it will select proper address pool by configuration, and then pick out a free IP address, which will sent out to the client together with other parameters (like DNS server address, address lease limit). Lots of standard configuration option is identified in RFC2132, where more detailed information can be got there. But most DHCP configurations use only a few options of the rules.

Following the steps below user can configure address pool:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp sever ip-pool WORD** *start-ip-address end-ip-address mask-address* **ip** *<0-14>* **[gateway** *ip-address*] **[dns** *ip-address*] **[secondary-dns** *ip-address*]	Configure the address pool
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp server ip-pool**	Show DHCP Server address pool configuration

Notice:

➢ The command can configure one address pool to IP interface once. If IP interface does not exist when configuring, still the address pool can be successfully configured, but it will not take effect until the IP port is created and the IP address is configured. If the IP port is changed or deleted, the configured address pool can still be kept. Once the IP port is re-created, the configured address pool will take effect again.

➢ If the client and the server is in the same subnet, when configuring IP address pool, the network section that the address pool is in should be the same with the network section that of IP port address's, that is to say, address pool's network address is the same with the port's network address;

if the client connects the server through DHCP Relay, then the server's address and relay-ip should be within the same network section. Otherwise, DHCP Server will not distribute IP address for DHCP client.

Use global configuration command **no ip dhcp server ip-pool** ip-pool to delete the configured address pool. If the IP address pool that is to be deleted does not exist, returned value is fault.

Here, the maximum IP address pool number that can be configured for each IP port is 4, the maximum IP address number that the switch supports is 2500. Address pool take the name as the only mark.

Configuration example:

Raisecom#**config**

Raisecom(config)#**ip dhcp server ip-pool** *pool1 192.168.1.100 192.168.1.200*

255.255.255.0 **ip** *4* **gateway** *192.168.1.1* **dns** *192.168.1.1* **secondary-dns** *10.168.0.1*

Raisecom(config)#**exit**

Raisecom#**show ip dhcp server ip-pool**

The result is shown below

--

Name of ip pool table : pool1

Status of IP pool table: active

IP address range: 192.168.1.100 - 192.168.1.200

Mask: 255.255.255.0

Including IP Interface: 4

IP address of gateway: 192.168.1.1

IP address of DNS server: 192.168.1.1

IP address of secondary DNS server: 10.168.0.1

--

Valid IP pool count : 1

Valid IP address count : 12

Allotted IP address count : 0

Gateway and dns is optical, if they are not used, default gateway and DNS will not be selected for the client.

27.2.2.6 Configure lease table timeout

When distributing IP address for the client, it is needed to designate the lease time of the IP address. By default the system lease time is:

1: default lease time: 30 minutes (usually it will not be used);

2: the maximum lease time: 10080 minutes (7days), when the lease time that the client requests is larger than this value, the larger value will be used.

3: the least lease time: 30 minutes, when the lease time that the client requests is smaller than this value, least lease time will be used; otherwise, according to the request time, if the client does not designate lease time, use the least lease time for distribution.

If the administrator needs to modify the least lease time, manual configuration is needed.

The configuration step is as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2 (optical)	**ip dhcp sever default-lease** *timeout*	Configure the IP address pool default lease time for DHCP server
3 (optical)	**ip dhcp sever max-lease** *timeout*	Configure the IP address pool maximum lease time for DHCP serve
4 (optical)	**ip dhcp sever min-lease** *timeout*	Configure the IP address pool least lease time for DHCP serve
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp server**	Show DHCP server configuration

Notice: The lease time configured here is used for all the IP address of the address pool. At the same time, the maximum lease time can not be shorter than least rent time, default lease time must be between maximum and least lease time.

Use global command **no ip dhcp server default, no dhcp-server max-lease, no dhcp-server min-lease** to cannel the current setting, and restore system default lease time setting.

Configuration example:

Raisecom#**config**

Raisecom(config)#**ip dhcp server default-lease** *60*

Raisecom(config)#**ip dhcp server max-lease** *1440*

Raisecom(config)#**ip dhcp server min-lease** *45*

Raisecom(config)#**exit**

Raisecom#**show ip dhcp server**

The result is shown below:

DHCP Server: Enabled

IP Interface Enabled: 4

Total Number: 1

Max lease time: 1440 m

Min lease time: 40 m

Default lease time: 60 m

27.2.2.7 Configure neighbour proxy IP address

When the client is connected with the server by DHCP Relay, DHCP server must know the neighbour DHCP Relay IP address, which needs the administrator's manual configuration as well.

The configuration step is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp sever relay-ip** *ip-address ip-mask*	Configure neighbour proxy IP address
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp server relay-ip**	Show DHCP server configuration

Notice: Only ISCOM3000 serious switches support the command **ip dhcp server relay-op.** Here the configured neighbour proxy IP address is actually the port address that is connected with the client, as is shown in the typical example. The maximum number of neighbour proxy IP address is 8.

Use global configuration command **no ip dhcp server relay-ip** ip-address to delete neighbour proxy IP address configuration.

Configuration example:

Raisecom#**config**

Raisecom(config)#**ip dhcp server relay-ip** *192.168.1.1 255.255.255.0*

Raisecom(config)#**exit**

Raisecom#**show ip dhcp server relay-ip**

The result is shown below:

index   IP address   IP Mask   Status

---

1   192.168.1.1   255.0.0.0   active

27.2.3 Monitoring and maintaining

Use different **show** commands to show the switch DHCP Server running and configuration situation for monitoring and maintaining. All the show commands are listed below:

Command	Description
show ip dhcp server	Show DHCP Server configuration and static information
show ip dhcp server ip-pool	Show DHCP Server address pool information
show ip dhcp server relay-ip	Show the configured neighbour DHCP proxy address information
show ip dhcp server lease	Show the designated IP address and the corresponding information

Notice：Only ISCOM3000 serial switches supports the command **show ip dhcp server relay-ip.** Before using **show ip dhcp server lease,** the system time should better be configured accurately, because lease time limit is computed according to the system date absolute time.

Use **show ip dhcp server** command to look over the configuration information, like global or IP port configuration information, static information or so.

Raisecom#**show ip dhcp server**

In English:

DHCP Server: Enabled

IP Interface Enabled: 4

Total Number: 1

Max lease time: 1000 m

Min lease time: 32 m

Default lease time: 300 m

Statistics information:

Running time: 0 hours 7 minutes 33 seconds

Bootps: 0

Discover: 0

Request: 0

Release: 0

Offer: 0

Ack: 0

Nack: 0

Decline: 0

Information: 0

Unknows: 0

Total: 0

Use the command **show ip dhcp server ip-pool** to show the configured address pool information:

Raisecom#**show ip dhcp server ip-pool**

Name of IP pool table: dhcp

Status of IP pool table: active

IP address range: 11.1.1.33 - 11.1.1.44

Mask: 255.255.255.0

Including IP Interface: 4

IP address of gateway: 0.0.0.0

IP address of DNS server: 0.0.0.0

IP address of secondary DNS server: 0.0.0.0

Valid IP pool count: 1

Valid IP address count: 12

Allotted IP address count: 0

Use the command **show ip dhcp server relay-ip** to show the configured neighbour proxy address information:

Raisecom#**show ip dhcp server relay-ip**

Index IP Address	*IP Mask*	*Status*
1 11.1.1.34	*255.255.255.0*	*active*

Use the command **show ip dhcp server lease** to show the configured neighbour proxy address information

Raisecom#**show ip dhcp server leas**e

IP Address	*Hardware Address*	*Lease Expiration*	*IP Interface*
172.16.1.11	*00:a0:98:02:32:de*	*Feb-01-2006 11:40:00*	*1*
172.16.3.254	*02:c7:f8:00:04:22*	*Jul-01-2006 23:00:00*	*1*

Character instruction:

IP Address: the client IP address;

Hardware Address: the client MAC address

Lease Expiration: lease timeout limit

IP Interface: IP interface number

Lease timeout limit is computed according to system date, format is mm-dd-yyy hh:mm:ss

27.2.4 Typical configuration example

The typical DHCP Relay and Server configuration case is show below:

  ✧   Direct connection to the client for IP address
  ✧   The client get IP address through proxy

1) Configuration instruction

The example is simple and typical in realizing DHCP protocol. Specific connection state is shown in fig 2-2. In the figure ISCOM3026, as DHCP Relay, divides the two VLAN: VLAN 10 and VLAN 20, the two corresponding subnet IP address are 192.168.1.10 and 172.168.1.10 respectively. The DHCP server is ISCOM3026A, IP address is 172.168.1.2, suppose the subnet NDS be 172.168.1.3, subnet 1and subnet 2 need to get connection to public network through gateway 172.168.1.1. To realize the client accessing the resource of the public network, it is only needed to configure DHCP Server and DHCP Relay correctly.

2) Topology figure
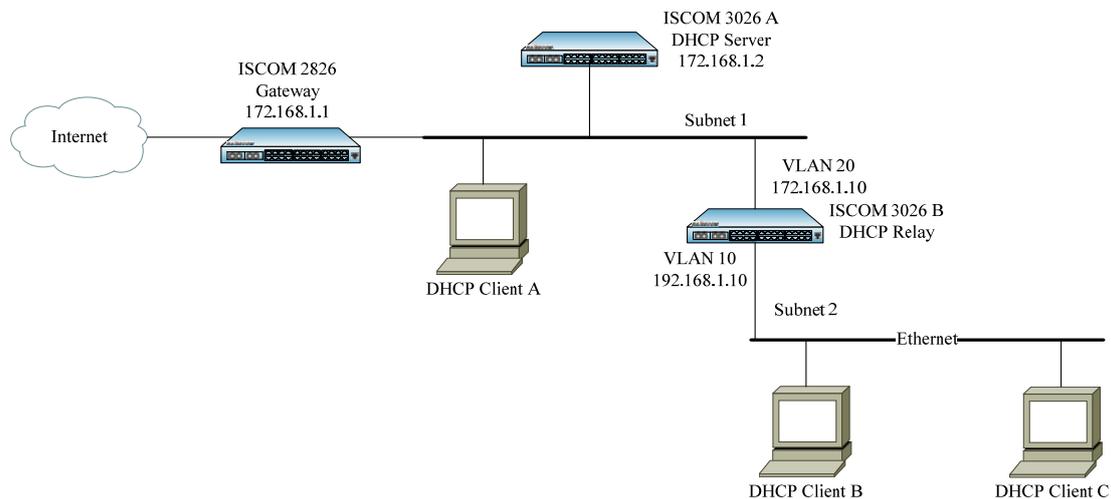
Fig 2-2 typical configuration example

3) Configuration steps

Configure DHCP Server:

➢ Configure VLAN and interfaces:

Raisecom(config)#**create vlan** *20* **active**

Raisecom(config)#**interface port** *1*

Raisecom(config-port)#**switchport access vlan** *20*

Raisecom(config-port)#**exit**

Raisecom(config)#**interface ip** *2*

Raisecom (config-ip)#**ip address** *172.168.1.2 255.255.0.0 20*

➢ Configure address pool

Configuring a address pool for both subnet 1 and subnet 2 respectively.

Raisecom (config)#**ip dhcp server ip-pool** *pool1 172.168.1.100 172.168.1.200 255.255.0.0* **ip** *2* **gateway** *172.168.1.1* **dns** *172.168.1.3*

Raisecom(config)#**ip dhcp server ip-pool** *pool2 192.168.1.100 192.168.1.200 255.255.255.0* **ip** *2* **gateway** *172.168.1.1* **dns** *172.168.1.3*

Raisecom (config)#**exit**

Raisecom #**show ip dhcp server ip-pool**

➢ Start DHCP Server service

Raisecom (config)#**ip dhcp server**

Raisecom(config)#**interface ip** *2*

Raisecom(config-ip)#**ip dhcp server**

Raisecom #**show ip dhcp server**

➢ Configure neighbour proxy IP address

Raisecom (config)#**ip dhcp server relay-ip** *192.168.1.10 255.255.255.0*

Raisecom (config)#**exit**

Raisecom #**show ip dhcp server relay-ip**

➢ Configure the router

Raisecom (config)#**ip route** *192.168.1.0 255.255.255.0 172.168.1.10*

➢ Configure DHCP Relay

Create VLAN and the interface

Raisecom (config)#**create vlan** *10* **active**

Raisecom (config)#**interface port** *1*

Raisecom(config-port)#**switchport access vlan** *10*

Raisecom(config-port)#**exit**

Raisecom (config)#**interface ip** *2*

Raisecom(config-ip)#**ip address** *192.168.1.10 255.255.255.0 10*

Raisecom (config)#**create vlan** *20* **active**

Raisecom (config)#**interface port** *2*

Raisecom(config-port)#**switchport access vlan** *20*

Raisecom(config-port)#**exit**

Raisecom (config)#**interface ip** *3*

Raisecom (config-ip)#**ip address** *172.168.1.10 255.255.0.0 20*

➢ Enable router function

Raisecom(config-ip)#**exit**

Raisecom(config)#**ip routing**

➢ Configure DHCP server IP address

Raisecom(config)#**ip dhcp relay ip-list** *2* **target-ip** *172.168.1.2*

Raisecom (config)#**exit**

Raisecom #**show ip dhcp relay**

➢ Start DHCP Relay

Raisecom (config)#**ip dhcp relay**

Raisecom(config)#**exit**

Raisecom #**show ip dhcp relay**

The client will be configured as auto acquiring IP address through DHCP

4) show the result

Show DHCP configuration static information, address pool information and the configured IP address information

On ISCOM3026A use the command **show ip dhcp server**、**show ip dhcp server ip-pool** and **show ip dhcp server lease**.

Show DHCP Relay information

On ISCOM3026B use the command **show ip dhcp relay**.

➢ Show client A

c:\>ipconfig /all

    Ethernet adapter: local connection:

      Connection-specific DNS Suffix   . :

      Description . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC

      Physical Address. . . . . : 00-50-8D-4B-FD-27

      DHCP Enabled. . . . . : Yes

       Autoconfiguration Enable. . . :Yes

      IP Address. . . . . : 172.168.1.100

      Subnet Mask . . . . : 255.255.0.0

      Default Gateway . . . . : 172.168.1.1

       DHCP server. . . . .: 172.168.1.2

      DNS Servers . . . . : 172.168.1.3

      Lease Obtained. . . . . : 13:03:24 Sep. 8, 2006

       Lease Expires. . . . . : 13:33:24 Sep. 8, 2006

➢ Show client B

c:\>ipconfig /all

    Ethernet adapter: local connection:

      Connection-specific DNS Suffix   . :

      Description . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC

      Physical Address. . . . . : 00-50-8D-4B-DE-46

      DHCP Enabled. . . . . : Yes

    Autoconfiguration Enable. . . :Yes

      IP Address. . . . . : 192.168.1.100

      Subnet Mask . . . . : 255.255.255.0

      Default Gateway . . . . : 172.168.1.1

➢ Show client C:

Client C is the same with client B in content, the IP address is 92.168.1.101

27.3 DHCP Relay Configuration

This chapter is mainly about how to configure and maintain DHCP Relay on the switch, including:

- ✧ DHCP Relay principle overview
- ✧ DHCP Relay configuration
- ✧ Monitoring and maintaining
- ✧ Typical configuration example
- ✧ DHCP Relay trouble shooting

27.3.1 DHCP Relay principle overview

Early DHCP protocol is suitable for only the situation that the client and server are in the same subnet, which can not go through network sections. Therefore, for dynamical host configuration, configuring a DHCP server on all the network sections is needed, which is obviously wasteful.

The introduction of DHCP Relay solves this problem: the local network client can communicate with the other subnet DHCP servers by DHCP Relay, and get the legal IP address finally. Thus, the DHCP client on several networks can use the same DHCP server, which decreases the cost and helps centralized management

DHCP Relay provides DHCP broadcast message transparent transmission function, which is able to transmit the broadcast message of DHCP client (or server) transparently to the other network section DHCP server (or client).

In the process that DHCP Relay completes dynamic configuration, the processing way that DHCP client and server takes is basically the same with that of not through DHCP Relay. The following steps are only about DHCP Relay transmission:

(1) DHCP client transmits DHCP-DISCOVER message in broadcasting.

(2) When the network equipment with DHCP Relay function receives the broadcast message, by configuration it will transmit the message to the specific DHCP server in unicast.

(3) DHCP server makes IP addresses distribution, and sends the configuration information to the client through DHCP Relay.

Usually, DHCP Relay can be either host or three-layer switch or router, if only DHCP Relay service program is enable.

The figure below is a typical DHCP Relay application:
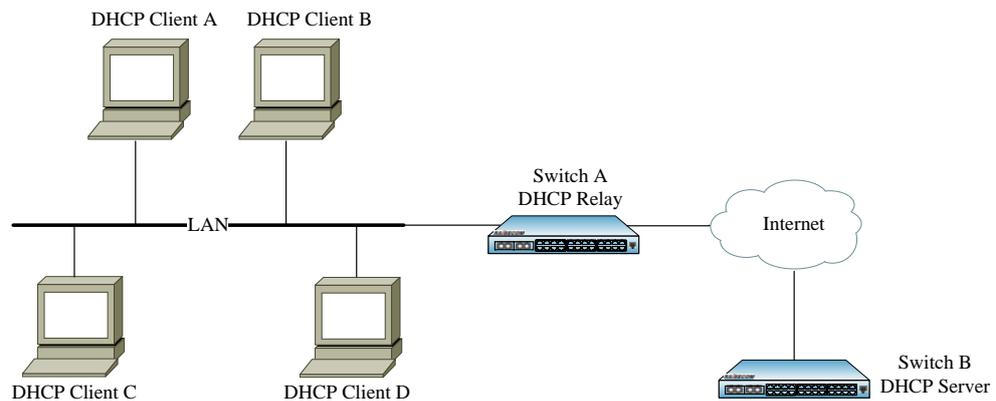
Fig 3-1 DHCP Relay typical application

The mechanism of DHCP Relay support Option 82 is shown below:

(1) DHCP client sends out request message in the form of broadcasting when initialized.

(2) The DHCP Relay equipment that is connected with local network will receive the broadcast message, check out if there has been Option 82 in the message, and handles it in the corresponding way.

(3) If there has been Option 82 in the message, the equipment will follow the configured strategy to handle the message (drop, replace the Option 82 in the message that has been there with the relay equipment's Option 82 or keep the Option 82 that has been there), and transmits the request message to DHCP server.

(4) If there is no Option 82 in the request message, the Option 82 of DHCP equipment will be added into the message (located in the end of all the options) and be transmitted to DHCP server. At this time, the Option 82 of the request message contains the port number of the switch which is connected with DHCP client, the number of the VLAN that the port belongs to and the DHCP Relay equipment's own MAC address and so on.

(5) When DHCP server receives the DHCP request message that is transmitted by DHCP Relay equipment, it will record the information from Option in the message, then transmit the message that contains DHCP configuration information and Option 82 information.

(6) After DHCP Relay receives the response message of DHCP server it will peel off the message's Option 82 information, then transmit the message that contains DHCP configuration information to DHCP client.

Explanation: there are two sorts of request messages from DHCP client, DHCP-DISCOVER and DHCP-REQUEST message. Because of the different mechanisms that different manufacturers' DHCP server handle request messages, some equipments handle DHCP-DISCOVER message's Option 82 information, while some others handle DHCP-REQUEST message's Option 82 information, so DHCP Relay handles both the two messages in the strategy of Option 82.

Otherwise, if DHCP Relay receives the messages sent out from the two DHCP client DHCP-DECLINE and DHCP-INFORM, it will handle Option 82 uniformly according to the strategy, without affecting its basic function of supporting Option 82.

27.3.2 Configure DHCP Relay

This part is about how to configure DHCP Relay on the switch, including the following configuration information:

- ✧ Default DHCP Relay configuration
- ✧ DHCP Relay configuration guide

◇ Global DHCP Relay configuration

◇ IP port DHCP Relay configuration

◇ DHCP Relay support Option 82 configuration

◇ DHCP Relay's handling strategy to the request messages that contains option 82 configuration

◇ Port DHCP Relay trust configuration

27.3.2.1 Default DHCP Relay configuration

The following table is the default configuration steps of DHCP Relay:

Function	Default value
Global DHCP Relay state	Disabled
IP port DHCP Relay state	Enabled
IP port's destination IP address	N/A
DHCP Relay support Option 82	Disabled
The strategy of DHCP Relay handling option 82 request messages	Replace
Port DHCP Relay trust	Untrusted

27.3.2.2 DHCP Relay configuration guide

1. Make sure the DHCP Snooping on the switch is not started;

2. Global DHCP Relay must be started;

3. If on a IP port DHCP Relay is not started, it can not work on this IP port;

4. When DHCP Relay is on, DHCP Snooping can not be started either on the switch;

5. Make sure the DHCP server that is connected with DHCP Relay has correct configuration and connection to the client. DHCP server must be ISCOM 3000 serious switches. Except making sure the correct configuration of IP port addresses and address pool, correct configuration to the neighbour proxy address and Relay addresses;

6. If the client acquires IP address automatically from DHCP server through multiplex Relay, you must make sure the connection of each equipment and correct configuration. The DHCP Relay number between the client and server, can not exceed 16 in RFC1542 rules, it is usually suggested not to exceed 4.

27.3.2.3 Configure global DHCP Relay

By default, global DHCP Relay is off. Only when global DHCP Relay is on can the switch DHCP Relay takes effect. User can take the following steps to start global DHCP Relay.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp relay**	Start global DHCP Relay
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp relay**	Show DHCP Relay configuration

Notice: If the switch starts DHCP Snooping, it can not start global DHCP Relay. On the opposite, if the switch starts global DHCP Relay, it can not start DHCP Snooping.

Use global command **no ip dhcp relay** to disable global DHCP Realy.

27.3.2.4 Configure IP port DHCP Relay

By default, IP port DHCP Relay function is on, user can use IP port command **no ip dhcp relay** to disable IP port DHCP Relay function. To start IP port DHCP Relay, use IP port command **ip dhcp relay.**

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** *4*	Enter IP port 4 configuration mode
3	**ip dhcp relay**	Start DHCP Relay
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp relay**	Show DHCP Relay configuration

Notice: When global DHCP Relay is off, on a certain IP port DHCP Relay can be started in advance. But only when global DHCP Relay starts can the DHCP Relay started on this port takes effect.

27.3.2.5 Configure IP port destination IP address

When the client equipment and DHCP server is not in the same broadcasting domain, the relay equipment in the middle must be able to transmit the kind of broadcasting packet. Configuring the destination IP address of DHCP Relay points out the destination address of the DHCP broadcasting packet from DHCP client for the relay equipment.

When DHCP Relay is configuring destination IP address, use network port LIST for the convenience of user's configuration. That is to say, according to the actual need, one command can be used to configure the same IP address for parts of the network ports or all the ports.

When DHCP Relay is configuring destination IP address, except the configuration commands in config mode, you can also configure the port's corresponding destination IP address in IP port, which is flexible.

Take the following steps to configure the port's destination IP address.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp relay ip-list all target-ip** *10.199.0.200*	For all the IP ports configure the destination IP 10.199.0.200
3	**ip dhcp relay ip-list** *1-3* **target-ip**	For IP port 1-3 configure the destination IP 10.200.0.200
4	**interface ip** *3*	Enter IP port 3 configuration mode
5	**ip dhcp relay target-ip**	Configure the destination IP 10.201.0.200
6	**exit**	Return to global configuration mode

Note:

➢ Here, the configured maximum destination IP address number for each port is 4. At the same time, make sure that the destination IP address is correct.

➢ When it comes to configuring destination IP address for several IP ports in one command, if configuring the destination IP address in a certain port fails, the rest IP port destination IP address configuration should be continued and return the cue which specific port configuring destination IP address fails, the format is: IP interface %s set target IP address unsuccessfully. Use IP table to replace %s in actual use. If only one port is configured successfully, the command line will return 'configuration successful' finally.

Use global configuration command **no ip dhcp relay ip-list target-ip** to delete the configured destination IP address of the IP port, or IP interface configuration command **no ip dhcp relay target-ip** in the corresponding port configuration mode.

Configuration example:

Raisecom#**config**

Raisecom(config)# **ip dhcp relay ip-list all target-ip** *10.199.0.200*

Raisecom(config)# **ip dhcp relay ip-list** *1-3* **target-ip** *10.200.0.200*

Raisecom(config)#**interface ip** *3*

Raisecom(config-ip)#**ip dhcp relay target-ip** *10.201.0.200*

Raisecom(config-ip)#**exit**

Raisecom(config)#**exit**

Raisecom#**show ip dhcp relay**

The result is shown below:

DHCP Relay: Enabled

IP Interface   Enabled Status   Target IP Address

--

0   enabled   10.199. 0.200

1   enabled   10.199. 0.200

10.200.0.200

2   enabled   10.199. 0.200

10.200.0.200

3	*enabled*	*10.199. 0.200*
		10.200.0.200
		10.201.0.200
4	*enabled*	*10.199. 0.200*
...	*...*	*...*

27.3.2.6 Configure DHCP Relay support option 82

By default, DHCP Relay do not support option 82, in global configuration mode use **ip dhcp relay information option** to start DHCP Relay support option 82.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp relay information**	Start DHCP Relay support option 82
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp relay information**	Show DHCP Relay support Option 82 configuration information and port trust list

Notice: To active DHCP Relay support option 82, enable global DHCP Relay service first. To make option 82 function available, corresponding configuration on DHCP Server is needed.

Use global configuration command **no ip dhcp relay information option** to disable DHCP Relay support Option 82.

27.3.2.7 Configure DHCP Relay request message handling strategy

By default, DHCP Relay handling strategy to the client request messages is Replace, that is to fill Option 82 in the way of normal or verbose, replace the Option 82 contents that has been there and transmit it. In global configuration mode use the command **ip dhcp relay information policy {drop| keep | replace}** to configure the message handling strategy of DHCP Relay as drop, keep or replace.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp relay information policy** {*drop* / *keep* / *replace*} [**schedule-list** *list-no*]	Configure DHCP Relay request message handling strategy
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp relay information**	Show DHCP Relay handling strategy to client request message

Notice: The command configured request message handling strategy can available only in DHCP Relay support Option 82.

Use global configuration command **no ip dhcp relay information policy {drop | keep | replace}** **[schedule-list** *list-no*] to recover default DHCP Relay handling strategy to Option 82.

The configuration example:

Raisecom#**config**

Raisecom(config) **ip dhcp relay information policy keep**

Raisecom(config)#**exit**

Raisecom#**show ip dhcp relay information**

The result is shown below:

Option 82: Enabled

Policy: Keep

Port   Trusted

...   ...

27.3.2.8 Port DHCP Relay trust configuration

By default, if one DHCP message gateway address part is 0 and relay agent information option part (option 82) exists, then DHCP Relay will drop messages of this kind. If DHCP Relay is required to transmit messages of this kind, use the command to configure DHCP Relay port trust. After the specific port has configured DHCP Relay port trust command, these port can transmit this kind of DHCP messages normally. You can also use the key word all to set all the system port Relay Agent Information Option port trust.

When configuring port trust, except the configuration commands in config mode, you can configure the port trust state under the port directly as well, which is flexible.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp relay information trusted port-list** *1-7*	Set port 1-7 to trusted port
3	**interface ip** *8*	Enter port 8 configuration mode
4	**ip dhcp relay information trusted**	Configure the destination IP 10.201.0.200
5	**exit**	Return to global configuration mode
6	**exit**	Return to privileged EXEC mode
7	**show ip dhcp relay information**	Show DHCP Relay support Option 82 configuration information and port trust table

Notice: Only when DHCP Relay support Option 82 can port trust take effect.

Use global configuration command **no ip dhcp relay information port-list** to set the port to distrust port,

in the corresponding port configuration mode use port configuration command **no ip dhcp relay information option** to realize it.

Configuration example:

Raisecom#**config**

Raisecom(config) **ip dhcp relay information trusted port-list** *1-7*

Raisecom(config)#**interface ip** *8*

Raisecom(config-port)# **ip dhcp relay information trusted**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show ip dhcp relay information**

The result is shown below:

Option 82: Disabled

Policy: Replace

Port   Trusted

----

1   yes

2   yes

3   yes

4   yes

5   yes

6   yes

7   yes

8   yes

...   ...

27.3.3 Monitoring and maintaining

Use different show commands to show switch DHCP Relay running state and configuration state for monitoring and maintaining. All the show commands are listed below:

Command	Description
show ip dhcp relay	Show DHCP Relay configuration information
show ip dhcp relay statistics	Show DHCP Relay static.
show ip dhcp relay information	Show the configured neighbour DHCP proxy address information

Use the command **show ip dhcp relay** to show HDCP Relay basic configuration information, including DHCP Relay state, IP port DHCP Relay state and the corresponding DHCP proxy destination IP address.

Raisecom#**show ip dhcp relay**

DHCP Relay: Enabled

IP Interface   Enabled Status   Target IP Address

----

0   enabled   10.199. 0.200

1   enabled   10.199. 0.200

10.200.0.200

2   enabled   10.199. 0.200

10.200.0.200

3   enabled   10.199. 0.200

10.200.0.200

10.201.0.200

4   enabled   10.199. 0.200

...   .

Use the command **show ip dhcp relay statistics** to show DHCP Relay static, including DHCP Relay running time and received/sending messages number.

Raisecom#**show ip dhcp relay ip-pool**

Runtime: 0 hours 23 minutes 34 seconds

Packet Type   Receive   Send

Bootp   0   0

Discover   1   1

Request   1   1

Decline   0   0

Offer   0   0

Ack   0   0

Nack   0   0

Decline   0   0

Inform   0   0

Unknowns   0   0

Total   2   2

Use the command **show ip dhcp relay information** to show HDCP Relay support Option 82 configuration

information and port trust table:

Raisecom#**show ip dhcp relay information**

In English:

Option 82: Enabled

Policy: Replace

Port	*Trusted*
1	*yes*
2	*no*
3	*yes*
4	*yes*
...	*...*

Instruction:

DHCP Relay supporting Option 82 includes:

a) Enabled

b) Disabled

The strategy includes:

a) Drop

b) Keep

c) Replace

27.3.4 Typical configuration example

DHCP Relay typical configuration example is like DHCP Server typical configuration example. The following is about a example that the client using DHCP Snooping connects to DHCP Relay and get IP address.

1) Configuration instruction

1: the connection of starting Snooping on DHCP Snooping equipment is as fig 3-2, start DHCP Snooping support option 82, and set port 2 to DHCP Snooping trust port.

2: DHCP Relay divides two subnets, the connection between it and the client and the server connection and configuration is as the figure below. Follow the figure to configure VLAN, IP port address and the VLAN that the port belongs to.

3: DHCP Server divides two subnets, establish correct address pool (10.150.0.2 – 10.150.0.100) on the subnet, start DHCP Server function at the same time and configure relay-ip shown in the figure (consult DHCP Server module configuration guide). Then follow the figure to configure VLAN, IP port address and VLAN the port belongs to, and configure it to the router belongs to 10.150 network segment.

4: set PCI to auto acquiring IP address.

2) Topology figure
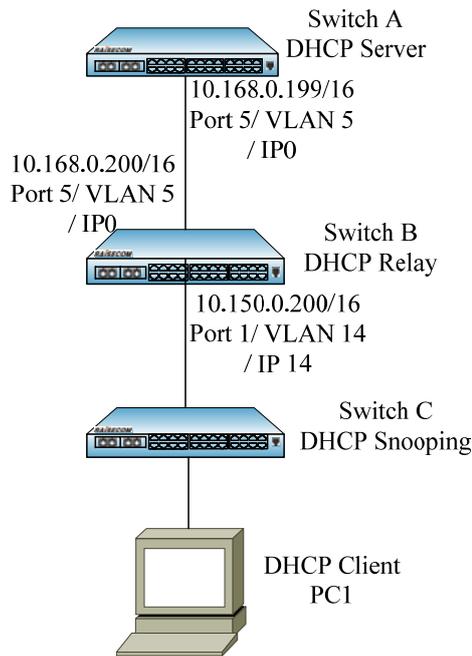
Fig 3-2 typical configuration example

3) Configuration steps:

Configure DHCP Relay:

Start global DHCP Relay

Raisecom (config)#**ip dhcp relay**

Prot 14 configure destination IP addresss

Raisecom (config)# **ip dhcp relay ip-list** *14* **target-ip** *10.168.0.199*

Start DHCP Realy support option 82

Raisecom (config)**ip dhcp relay information option**

Configure port 1 as DHCP Relay trust port

Raisecom (config)**ip dhcp relay information trusted port-list** *1*

Open the router function

Raisecom (config)#**ip dhcp relay ip routing**

a) show the result

Show the client PC1

C:\>ipconfig /all

Ethernet adapter local connection

    Connection-specific DNS Suffix   . :

    Description . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC

    Physical Address. . . . . : 00-50-8D-4B-FD-27

    DHCP Enabled. . . . . : Yes

Autoconfiguration Enable. . . :Yes

IP Address. . . . . : 10..150.0.0

Subnet Mask . . . . : 255.255.0.0

Default Gateway . . . . :

DHCP server. . . . .: 10.168.0.199

DNS Servers . . . . :

Lease Obtained. . . . . : 13:03:24 April 8, 2007

Lease Expires. . . . . : 13:33:24 April 8, 2007

27.3.5 DHCP Relay trouble shooting

1. If the correct destination IP address is not designated, DHCP Relay can not transmit the message correctly.

2. If the gateway address field of a DHCP message is 0 and relay agent information option field exists, DHCP Relay distrusted port will drop messages of this kind.

If the configuration above still can not help, please examine if DHCP Relay has started router function, and examine if DHCP server address is correctly configured, if the neighbor proxy default gateway or router is configured.

27.4 DHCP Option Configuration

This chapter is mainly about how to configure and maintain DHCP Option, including:

- ✧ DHCP Option principle overview
- ✧ DHCP Option configuration
- ✧ Monitoring and maintenance
- ✧ Typical configuration example
- ✧ DHCP Option trouble shooting

27.4.1 DHCP Option principle overview

There are kinds of request options in DHCP request messages, while one special option exists in DHCP snooping, DHCP relay, DHCP server request and answer messages, which is used to mark the client's position. This option is OPTION82, including two sub-options: circuit-id and remote-id. With the two sub-options, the server is able to acquire the position information of the client and take effective management.

27.4.2 DHCP Option configuration

This part is about how to configure DHCP OPTION on the switch, including:

Default DHCP OPTION configuration

DHCP OPTION configuration guide

Global DHCP OPTION attach-string configuration

DHCP OPTION circuit-id configuration in port mode

DHCP OPTION remote-id configuration in global mode

1.4.2.1 Default DHCP OPTION configuration

The table below lists the default DHCP OPTION configuration:

Function	Default value
Global attach-string configuration	Empty
Global remote-id configuration	switch-mac
In port mode circuit-id	Empty

27.4.2.2 DHCP OPTION configuration guide

If the equipment supports DHCP Snooping or DHCP Relay, then DHCP Option module can be configured on it.

27.4.2.3 Configure global DHCP OPTION attach-string

By default, global DHCP OPTION attach-string is empty, and the value will be the configured value after configuration. The format of option 82 sub-option 1 in DHCP OPTION message is:

Port number/VLAN ID/attach-string

Configuration steps:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp information option attach-string** *raisecom*	Configure DHCP OPTION attach-string to raisecom
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp information option**	Show DHCP OPTION module configuration

27.4.2.4 Configure DHCP OPTION circuit-id in port mode

By default, port circuit-id is empty, and the value will be the configured value after configuration. The format of option 82 sub-option 1 in DHCP OPTION message is:

Circuit-id

The configuration steps:

Step	Command	Description
1	**config**	Enter global configuration mode

2	**interface port 10**	Enter port 10 configuration mode
3	**ip dhcp information option circuit-id** *raisecom*	Configure port 10 circuit-id to raisecom
4	**exit**	Return to global configuration mode
5	**exit**	Return to privilege EXEC mode
6	**show ip dhcp information option**	Show DHCP OPTION module configuration

27.4.2.5 Configure DHCP OPTION remote-id in global configuration mode

By default, remote-id mode is switch-mac mode, when this option is configured, DHCP OPTION82 can be sent out in the configured mode.

Switch-mac: remote-id will be sent out in the form of switch MAC address binary system;

Client-mac: remote-id will be sent out in the form of client equipment MAC address binary system;

Switch-mac-string: remote-id will be sent out in the form of switch MAC address character string;

Client-mac-string: remote-id will be sent out in the form of client MAC address character string.

The configuration steps:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip dhcp information option remote-id switch-mac-string**	Configure remote-id being sent out in the form of switch MAC address character string
3	**exit**	Return to privileged EXEC mode
4	**show ip dhcp information option**	Show DHCP option module configuration

27.4.3 Monitoring and maintenance

Use **show** to show the switch DHCP OPTOIN configuration

Command	Description
show ip dhcp information option	Show DHCP OPTION configuration

Use **show ip dhcp information option** to show basic DHCP OPTION configuration, including global DHCP OPTION82 sub-option circuit state, circuit-id configuration in port mode, remote-id configuration mode.

Raisecom#**show ip dhcp information option**

Switch use attach string as circuit ID

attach-string: raisecom

remote ID use switch MAC-address as string mode

27.4.4 Typical configuration example

If the carrier do not configure OPTION module

If the carrier do not configure DHCP OPTION, the switch will mark the client device position in default way

If the carrier wants to mark the client device position

If the carrier wants to mark the client device position in the way of attach-string

Configure attach-string in global configuration mode

Raisecom(config)#**ip dhcp information option attach-string** *STRING*

The client position information is as follows:

Port number\VLAN\STRING MAC address (the carrier can choose MAC address mode)

If the carrier wants to mark client device position completely in its own way

In port configuration mode, the carrier is able to mark the client position in its own way, for example, one carrier needs the client mark shown as follows:

Option 1

*<Access-Node-Identifier>/**PON**/<rack> / <shelf> / <slot> / <PON> : <ONT> . <ONT-slot> . <UNI>*

<Access-Node-Identifier>

<rack>

<shelf>

<slot>

<PON>

<ONT>

<ONT-SLOT>

<UNI>

Circuit-id can be configure to the needed format in port mode, the steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port 10**	Enter port 10 configuration mode
3	**ip dhcp information option circuit-id** *CHINA/PON/1/1/08/01:28.1.10*	Configure port 10 circuit-id to CHINA/PON/1/1/08/01:28.1.10
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp information option**	Show DHCP OPTION module configuration

27.4.5 DHCP OPTION trouble-shooting

N/A

Chapter 29   802.1x

28.1 802.1x principle overview

802.1x module is based on IEEE802.1x protocol, or port based network access control technology, it makes authorization and control to access equipments on the equipments' physical access layer, and defines the point-to-point connection mode between the access equipment and access port.

The system structure of IEEE 802.1x includes three parts:

✓ Supplicant

✓ Authenticator

✓ Authorization Server

LAN access control equipment (like access switch) needs the Authenticator of 802.1x; user side equipment, like computer, needs to install 802.1x client (Supplicant) software (or the 802.1x client pre-positioned in Windows XP); while 802.1x Authorization Server System usually stays in operator's AAA centre.

Authenticator and Authorization Server exchange information using Extensible Authorization Protocol; while Supplicant and Authenticator use EAPOL (EAP over LANs, defined in IEEE802.1x) for communication, the authorization data is encapsulated in EAP frame. The authorization data is encapsulated in the message of other AAA upper layer protocol (like RADIUS) so that it is able to go through complicated network and reach Authorization Server, this process is called EAP Realy.

The figure below is 802.1x system structure:
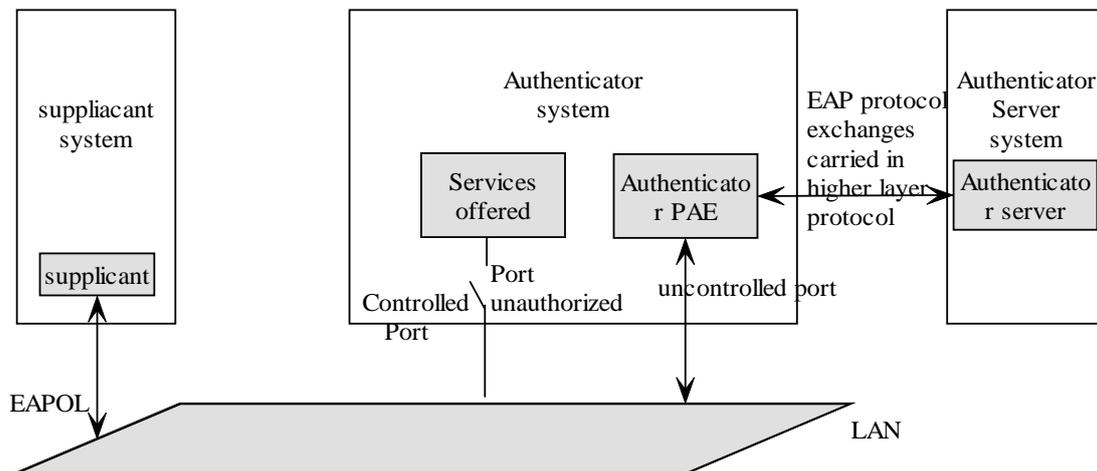
Fig 1: 802.1x system structure

'port based network access control' means to do authorization and control to the access equipments in LAN access control equipment port layer. If the user equipment connected to the port can go through the authorization, then it is able to visit the resources in LAN; if it can not pass the authorization, then it can not visit the network resources through switch – same as physical link down.

28.2 Configure 802.1x

802.1x configuration includes:

1. Default 802.1x configuration situation;

2. Enable/disable 802.1x global feature and port feature;

3. Configure RADIUS server IP address and RADIUS public key;

4. Show RADIUS server configuration;

5. Configure port access control mode;

6. Enable/disable 802.1 x reauthorization function;

7. Configure 802.1x reauthorization period;

8 Configure 802.1x silence time;

9. Configure Request/Identity resending period;

10. Configure Request/Identity resending period;

11. Configure RADIUS server overtime.

28.2.1 Default 802.1x configuration

Function	Default value
Global 802.1x feature	disable
Port 802.1x feature	disable
Port access control mode	auto
RADIUS server overtime	100s
802.1x reauthorization function	disable
802.1x reauthorization period	3600s
802.1 silence time	60s
Request/Identity resending period	30s
Request/Challenge resending period	30s

28.2.2 Basic 802.1x configuration

The basic 802.1x configuration is shown below:

✓   Enable/disable 802.1x global feature and port feature;

✓   Configure RADIUS server IP address and RADIUS public key;

✓   Configure port access control mode.

1. Enable/disable 802.1x global feature and port feature;

802.1x feature includes global 802.1x feature and port 802.1x feature, if one of them is not enabled, it will lead to 802.1x feature shown as constraint authorization passing through. 802.1x protocol and spanning tree

protocol (STP) can not be opened at the same time in the same port.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**dot1x** { **disable** | **enable** }	Enable/disable global 802.1x feature
3	**interface** { **port** | **line** | **client**} *<1- MAX_PORT_NUM >*	Enter ethernet physical port mode *1- MAX_PORT_NUM* the equipment port
4	**dot1x** { **disable** | **enable** }	Enable/disable port 802.1x feature
5	**exit**	Return to global configuration mode
6	**exit**	Return to privileged EXEC mode
7	**show dot1x** { **port-list** | **line** | **client**} *portlist*	Show physical port 802.1x configuration information *Portlist* use '_' and ',' to input more ports number

Notice:

➤ If a port has enabled STP and 802.1x protocol port can not be opened successfully, we need to disable port STP first.

➤ 802.1x protocol is physical port based access control protocol, it is not suggested that user enable 802.1x feature on aggregation port and not-Access port. When several users connects to the same switch port using shared network, if one user passes the authorization, then other users do not need authorization before they visit the network, but in this situation several user doing authorization at the same time may cause unsuccessful authorization because of interaction.

2. Configure RADIUS server IP address and RADIUS public key:

Configuring RADIUS server IP address and RADIUS public key is a necessary precondition of 802.1x port authorization.

The configuration steps are as follows:

Step	Command	Description
1	**[no] radius** *ipaddress*	Configure RADIUS server IP address
2	**[no] radius-key** *string*	Configure RADIUS server public key
3	**show radius-server**	Show RADIUS server configuration information

3. Configure port access control mode:

Port access control mode can be divided into three states: auto, authorized-force, unauthorized-force. By default it is auto. When global 802.1x feature and port 802.1x feature is on, the configuration determines directly if the authorization process will use authorized-force, unauthorized-force or protocol control mode.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface { port | line | client}** *<1-MAX_PORT_NUM >*	Enter ethernet physical port mode *1- MAX_PORT_NUM* equipment port
3	**dot1x auth-control {***auto/ authorized-force/ unauthorized-force***}**	Configure port control mode
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show dot1x** *{port-list | line | client} portlist*	Show physical port 802.1x configuration information *portlist*: use '_' and ',' to input more port numbers.

28.2.3 802.1x reauthorization configuration

Reauthorization function is for authorized users, so you should make sure that global and port 802.1x feature are enabled. By default reauthorization function is disabled. The authorized port keeps the state of authorized in the process of authorization; if reauthorization failed, then the port will enter unauthorized state.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** *{port | line | client}* *<1-MAX_PORT_NUM >*	Enter ethernet physical port mode *1- MAX_PORT_NUM* equipment port
3	**dot1x reauthentication** *{enable/disable}*	Enable/disable reauthorization function
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show dot1x** *{port-list/line/client} portlist*	Show physical port 802.1x configuration information *Portlist*, use '_' and ',' to input more port numbers

28.2.4 Configure 802.1x timer

In 802.1x authorization process, there are 5 timers related:

1. reauth-period: reauthorization overtime timer. In the time configured by the timer, 802.1x reauthorization will be raised. Reauth-period-value: the time length configured by reauthorization overtime timer, range is 1-65535, unit is second. By default it is 3600 seconds.

2. quit-period: quiet timer. When user authorization failed, the switch needs to keep quiet for a period of time, which is configured by quiet timer. When quiet timer exceeds the time it will make reauthorization. In quiet time, the switch will not process authorization messages. Quiet-period-value: the quiet time value configured by quiet timer, rang is 10-120, unit is second. By default, quiet-period-value is 60 seconds;

3. tx-period: transmission overtime timer. When the switch sends Request/Identity messages to user request end, the switch will start the timer, if in the configured time length user end software can not send request answering messages, the switch will re-send authorization request message, which will be sent three times. Tx-period-value: the time length configured by sending overtime timer, range is 10-120, unit is second. By default tx-period-value is 30 seconds.

4. supp-timeout: Supplicant authorized timeout timer. When the switch sends Request/Challenge message to user request end, the switch will start supp-timeout timer. if the user request end can not react in the time length configured in the timer, the switch will re-send the message twice. Supp-timeout-value: the time length configured by Supplicant authorization overtime timer, range is 10-120, unit is second. By default supp-timeout-value is 30 seconds.

5. server-timeout: Authentication Server. The timer defines the authenticator and the total overtime-length of RADIUS server dialog, when the timer exceeds the time the authenticator will end the dialog with RADIUS server, and start a new authorization process. The resending times and interval of RADIUS is determined by the switch RADIUS client. The switch RADIUS client message resend 3 times, while the waiting time is 5s. server-timeout-value: the overtime length configured by RADIUS server timer, range is 100-300, unit is second. By default server-timeout-value is 100s.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface { port	line	client}** *<1- MAX_PORT_NUM >*	Enter ethernet physical port mode
3	**[no] dot1x timer reauth-period** *reauth-period-value*	Configure reauthorization timer value Range is 1-65535, unit is second. By default the value is 3600s
4	**[no] dot1x timer quiet-period** *quiet-period-value*	Configure quiet-time timer value Range is 10-120, unit is second. By default quiet-period-value is 60s
5	**[no] dot1x timer tx-period** *tx-period-value*	Configure Request/Identity resending timer value Range is 10-120, unit is second. By default tx-period-value is 30s
6	**[no] dot1x timer supp-timeout** *supp-timeout-value*	Configure Request/Challenge resending timer value Range is 10-120, unit is second. By default supp-timeout-value is 30s
7	**[no] dot1x timer server-timeout** *server-timeout-value*	Configure RADIUS server overtime timer value Range is 100-300, unit is second. By default server-timeout-value is 100s
8	**exit**	Return to global configuration mode
9	**exit**	Return to privileged EXEC mode
10	**show dot1x { port-list	line	client}** *portlist*	Show physical port 802.1x configuration information Portlist, use '_' and ',' to input more port numbers.

28.2.5 802.1x statistics cleanup

Monitoring and port statistics information is used to count the EAPOL messages number for the switches and user end exchanging data. Cleaning port stat. will clean all the statistics information of the selected ports. The steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**clear dot1x{ port-list | line | client }** *portlist* **statistics**	Clear physical port 802.1x statistics information
3	**exit**	Return to privileged EXEC mode
4	**show dot1x { port-list | line | client}** *portlist* **statistics**	Show physical port 802.1x statistics information Portlist, use '_' and ','to input more port numbers.

28.2.6 Maintenance

Use **show** to show the configuration and running state of switch 802.1x function for the convenience of monitoring and maintenance.

The related **show** commands are shown below:

Commands	Description
show radius-server	Show RADIUS server configuration
show dot1x { port-list | line | client} *portlist*	Show physical port 802.1x configuration information
show dot1x { port-list | line | client} *portlist* **statistics**	Show physical port 802.1x statistics information

28.2.7 Configuration example

1. Configuration request:

➢ PC user can visit outer network after passing ARDIUS server authorization

➢ In authorization-force mode, PC needs not authorization before visiting outer network;

➢ In unauthorization-force mode, PC can not visit outer network;

➢ After passing authorization, PC will do reauthorization 600s later automatically.

2. Network structure:
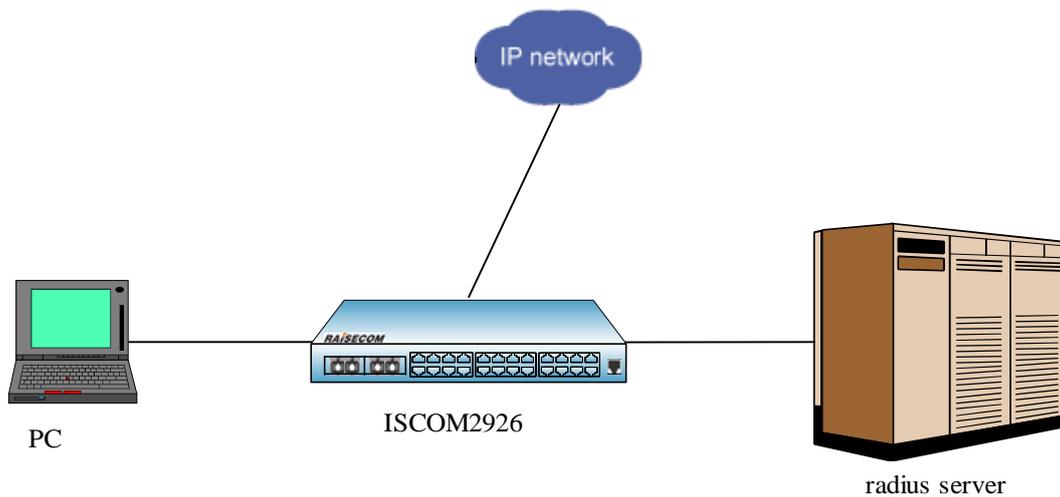
Fig 2: network structure

3. Configuration steps:

● Configure RADIUS server:

Follow ISCOM switch 802.1x user guide, add user raisecom in the server, the password is 123;

● Configure switch IP address and RADIUS server address:

Raisecom(config)#**interface ip** *0*

Raisecom(config-ip)#**ip address** *10.10.0.1 255.255.0.0 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**ip default-gateway** *10.10.0.2*

Raisecom(config)#**exit**

Raisecom# **radius** *192.168.0.1*

Raisecom# **radius-key** *raisecom*

● Configure enabling global and port 802.1x authorization function:

Raisecom(config)#**dot1**x *enable*

Raisecom(config)#**interface port** *1*

Raisecom(config-port)#**spanning-tree** *disable(STP and 802.1x are mutex)*

Raisecom(config-port)# **dot1x** *enable*

● PC end uses the client software for authorization request, username: raisecom, password: 123;

The PC client software will inform passing authorization, then we can visit outer network;

● Change the authorization mode to authorization-force mode:

Raisecom(config)#**interface port** *1*

Raisecom(config-port)#**dot1x auth-control authorized-force**

● PC end uses the client software for authorization request, username: raisecom, password: 123;

The PC client software will inform passing authorization, then we can visit outer network;

● Chang authorization-force mode to unauthorization-force mode

Raisecom(config)#**interface port** *1*

Raisecom(config-port)#**dot1x auth-control unauthorized-force**

● PC end uses the client software for authorization request, username: raisecom, password: 123;

The PC client software will inform passing authorization, then we can visit outer network;

● Enable reauthorization, and configure the time to 600s:

Raisecom(config)#**interface port** *1*

Raisecom(config-port)#**dot1x reauthentication** *enable*

● Show the statistics information:

Raisecom#**show dot1x port-list** *1* **statistics**

Notice: The switch's IP address, RADIUS server IP and key must well configured first of all;

Chapter 30   Auto-configuration And Load

29.1 Auto-configuration and load principle

Auto-configuration and load use TFTP protocol to acquire the configuration file stored on TFTP server, it is a way to configure the equipment. Viewing from application, it can be sorted to auto-run when the systems starts and running when the system is running.

Updated auto-configuration and load function allows the configuration files on TFTP server contain the commands related with auto-configuration and load function, so that there can be multi-configuration and load, to supply with the need of auto-configuration and load in complex network environment.

The switch supports several ways to make sure the configuration name on TFTP server correct, like manual input, using DHCP-Client for acquisition, using default configuration file name. Except this, user can specify one configuration file naming convention, using the attribute of the equipment to make sure the corresponding configuration file name by rules.

By combining multi-configuration and load technology and several accesses of acquiring configuration file name, the equipment can do auto-loading without configuration.

29.2 Default auto-configuration and load configuration

Function	Default value
TFTP server address	0.0.0.0 (not available)
The configuration files name on the server	Startup_config.conf
The naming rules of configuration files on the server	No rule number
Cover local configuration file switch state	Disable
On-power auto-configuration and load switch state	Disable
Send completing Trap switch state	Disable
Auto configuration and load running state	DONE
Auto configuration and load running result	NONE

29.3 Auto configuration and load function configuration

13.3.1 Configure TFTP server address

By default, TFTP server address is 0.0.0.0, 0.0.0.0 can not be configured by the command. Run the

opposite command **no service config tftp-server** and TFTP server address will be 0.0.0.0, but 0.0.0.0 can not be take as a available address to download configuration files and load it, and it shows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service config tftp-server** *A.B.C.D*	Configure TFTP server address
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show service config**	Show auto-configuration and load information, **Config server IP address** shows the configuration information of TFTP server address

To restore default address, use **no service config tftp-server**.

Notice:

> ➢ The configure IP address must accord with RFC1166, or it may cause configuration failure.
> ➢ After using the command to configure TFTP server address, when you run auto-configuration and load, the address that is configured by the command will be used, not the address acquired from DHCP Client. So, if you don't want to use local configured address, you don't have to configure it; if it has been configured, use **no service config tftp-server** to restore and run auto-configuration and load function.

13.3.2 Configure file name rule

By default, there is no filename naming rule, use **show service config** and it will show: --. When naming rule and filename are not configured, while no configuration filename is acquired successfully from DHCP Client function, the system will use default filename: **startup_config.conf**.

The configured file naming rule has the highest priority. When configured naming rule, you should use the naming rule to make sure the filename according to the equipment attribute.

Step	Command	Description
1	config	Enter global configuration mode
2	**service config filename rule** *[<80001-89999>]*	Configure file naming rules
3	**exit**	Quit from global configuration mode and enter privileged EXEC mode
4	show service config	Show auto-configuration and load information, among them, **Config filename rule** shows the filename configuration information

Use command **no service config filename rule** to delete the configured filename naming rules.

If there be no input rule number, then the system will create rule number in the way of question according to the answer user offers.

Raisecom(config)#**service config filename rule**

Enter the first question

Please check device type rule, configuration filename

0 - includes no device type information

1 - includes device type information

Please select:

0 means that the configuration files do not contain equipment type;

1 means that the configuration files do not contain switch type.

Input 0 or 1, press Enter, and enter the second question:

Notice: If the input number is not 0/1, it will be returned fault and failure in rule creation.

Please check MAC address rule, configuration filename

0 - includes no MAC address information

1 - includes the first 2 characters in MAC address

2 - includes the first 4 characters in MAC address

3 - includes the first 6 characters in MAC address

4 - includes the first 8 characters in MAC address

5 - includes the first 10 characters in MAC address

6 - includes all characters in MAC address

Please select:

0 means that ROS software version information is not contained in the configuration filename;

1 means that complete ROS software version information is contained in the configuration filename;

2 means that the software version information except the equipment type is contained in the configuration filename;

3 means that the software version information except the equipment type and date is contained in the configuration filename;

4 means that the software version high 3 figures are contained in the configuration filename;

5 means that the software version high 2 figures are contained in the configuration filename;

6 means that the software version the highest figure is contained in the configuration filename.

Input a random number among 0 and 6, press Enter, and end up rule number configuration.

Notice: If you input any number that is not among 0 and 6, it will return fault and failure in rule creation.

Please check MAC address rule, configuration filename

0 - includes no MAC address information

1 - includes the first 2 characters in MAC address

2 - includes the first 4 characters in MAC address

3 - includes the first 6 characters in MAC address

4 - includes the first 8 characters in MAC address

5 - includes the first 10 characters in MAC address

6 - includes all characters in MAC address

Please select:

Notice: If the input number belongs not to 0-6, it will be returned fault and failure in rule creation.

Please check ROS version rule, configuration filename

0 - includes no ROS version information

1 - includes entire ROS version information

2 - includes all except device type

3 - includes all except device type and date

4 - includes the highest 3 version number

5 - includes the highest 2 version number

6 - includes the highest version number

Please select:

Notice: If the input number belongs not to 0-6, it will be returned fault and failure in rule creation.

The configuration file naming rules are as follows:

The rule number is made up of 5 numbers, myriabit is 8, which has no actual meaning.

1) Kilobit shows the equipment type rules:

0 – equipment type is not included in the configuration file name;

1 – equipment type is included in the configuration file name;

2 – 9, reserved number, for rules extension.

2) Hundred shows MAC address rules: (take 000E08.5118 for example)

0 – the equipment MAC address information is not included in the configuration file name

1 – the first 2 characters of the equipment MAC address is included in the configuration file name (that is 00)

2 - the first 4 characters of the equipment MAC address is included in the configuration file name (000E)

3 - the first 6 characters of the equipment MAC address is included in the configuration file name (000E.5E)

4 - the first 8 characters of the equipment MAC address is included in the configuration file name (000E.5E08)

5 - the first 10 characters of the equipment MAC address is included in the configuration file name (000E.5E08.51)

6 - the first 6 characters of the equipment MAC address is included in the configuration file name (000E.5E.5E08.5118)

7 – 9 reserved number, for extension.

3) Tens show the software version number rule: (take ROS_4.3.2 ISCOM 2926.1.20080602)

0 – no software version information is contained;

1 – complete version information is contained (ROS_4.3.2 ISCOM 2926.1.20080602)

2 – the software version information without equipment type is contained (ROS_4.3.2.1.20080602)

3 – the software version information without equipment type and data is contained in the software version information (ROS_4.3.2.1)

4 – the software version information contains the higher three-figure (ROS_4.3.2)

5 – the software version information contains the higher two-figure (ROS_4.3)

6 – the software version information contains the higher one-figure (ROS_4)

7 – 9 restored, for extension.

4) Units digit shows the extension rules:

0 – extension rule is not supported;

1 – 9 restored, for extension.

The configuration file name is of the following style:

(equipment type)_M(MSC address)_(software version number)

For example: rule number 81650 stands for the configuration file name:

ISCOM2926_M000E.5E08.5118_ROS_4

Notice: After using the command to configure the naming rules, when auto-configuration is loaded, the naming rule will be used to configure the filename, while manual configuration filename and the one acquired from DHCP Client will no be used. So, if you do not want to use the naming rules, you don't have to configure the naming rules, and if it had been configured, use **no service config filename rule** to restore to default cases.

13.3.3 Configure the filename

By default, the filename is empty, use **show service config** and you will see: --. Follow the steps below to configure the filename, the length can not be longer than 80 bytes.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service config filename** *FILENAME*	Configure the filename. FILENAME: the filename, shorter than 80 bytes
3	**exit**	Quit from global configuration mode and enter privileged EXEC mode
4	**show service config**	Show auto-configuration loading information;

		config file name shows the configuration information of the filename.

Use **no service config filename** to delete the configured configuration filename.

Notice:

> ➢ If the configuration filename rule had been configured, then the configuration filename using this command will not be used.
> ➢ Under the promise that no naming rule is configured, if the command is used to configure the filename, then when auto-configuration is loaded, the filename configured by this command will be used, while the filename acquired from DHCP Client will not be used.
> ➢ If you want to use the filename acquired from DHCP Client or default filename, there is no need to configure the filename. And if it had been configured, use **no service config filename** to resume and run auto-configuration loading function.

13.3.4 Configure the switch of covering local configuration

Enable/disable covering local configuration file switch function. If it is enabled, use the file on the server to cover local configuration file in the process of auto-configuration loading.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service config overwrite** {*enable* | *disable*}	Configure the switch of overwriting local configuration file
3	**exit**	Return to global configuration mode and enter privileged EXEC mode
4	**show service config**	Show auto-configuration loading information, **config file name** show the configuration information of the filename

13.3.5 Run auto-configuration loading when the equipment is working

Use manual configuration to run auto-configuration loading, the configuration access is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service config**	Run auto-configuration loading function
3	**show service config**	Show the running state and result of auto-configuration loading, **operation states** shows the state of auto-configuration loading, **result** shows the result of auto-configuration loading

Notice: When the command is running, the switch of sending Trap when configuration is loaded successfully will be closed automatically.

13.3.6 Running auto-configuration loading automatically when the equipment is started

There are two situations when running auto-configuration loading automatically when the equipment is started:

1) The local configuration file of the equipment does not exist, then auto-configuration loading will be carried out automatically when the equipment is started

2) The local configuration file of the equipment exists, and **service config** exists in local configuration file, then auto-configuration loading will be started when local configuration file is loaded

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service config startup enable**	Enable auto-configuration loading when powered
3	**write**	Write the configuration into local configuration file
4	**exit**	Quit from global configuration mode and enter privileged EXEC moe
5	**reboot now**	Restart the switch

13.3.7 Stop auto-configuration loading try

If auto-configuration loading failed the switch will run auto-configuration loading once in a certain interval. The first failure interval is 2 seconds, the second time it is 10 seconds, the third time it is 100 seconds, the fourth time it is 300 seconds.

Use **no service config** to stop auto-configuration loading try caused by auto-configuration loading failure.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**no service config**	Stop auto-configuration loading try caused by loading failure
3	**exit**	Quit from global configuration mode and enter privileged EXEC mode

29.4 Monitoring and maintenance

Use **show service config** to show auto-configuration loading information and the running situation.

The information shown is as follows:

Perform on startup: disable

Config server IP address: --

Config file name rule: 81000

Config file name: --

Overwrite local configuration file: disable

Send Completion trap: disable

Operation states: done

Result: none

Use the command below to show the meaning of the configuration filename rule:

Command	Description
show service config filename rule [*ruleNum*]	Describe the meaning of filename rule, and provide the optical auto-configuration loading command rule number.

29.5 Typical configuration example

13.5.1 Destination

When the switch is started, by running auto-configuration loading twice, the switch can go through VLAN and get the specific configuration file.

13.5.2 The topology structure

The topology structure is shown below:
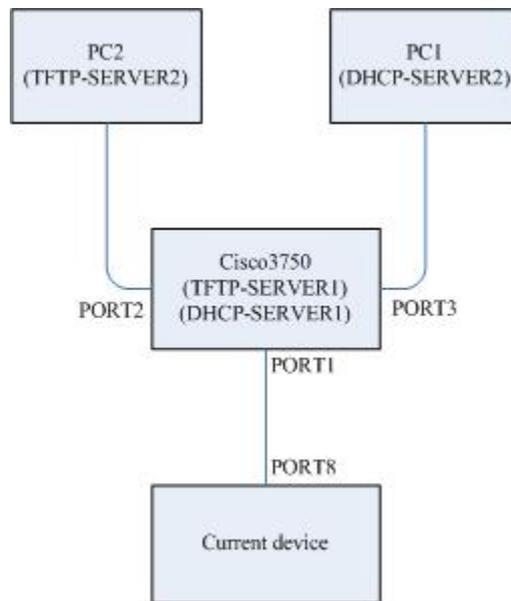
Fig 1 topology structure

13.5.3 The configuration steps on Cisco 3750

Step 1: configure IP address on VLAN port 100:

Switch#config

Switch(config)#interface vlan *100*

Switch(config-if)#ip address *20.100.0.100 255.255.255.0*

Switch(config-if)#no shutdown

Switch(config-vlan)#exit

Step 2: configure TFTP-SERVER1

Switch(config)#tftp-server flash:*startup_config.conf*

Step 3: configure DHCP-SERVER1 on VLAN 100:

Switch(config)#ip dhcp pool *newpool*

Switch(dhcp-config)#network *20.100.0.100 255.255.255.0*

Switch(dhcp-config)#option *150* **ip** *20.100.0.100*

Switch(dhcp-config)#exit

Step 4: configure port 2 to access mode and enter VLAN 200

Switch(config)#interface *G 1/0/2*

Switch(config-if)#switch mode access

Switch(config-if)#switch access vlan *200*

Switch(config-if)#exit

Step 5: configure port 3 to access mode and enter VLAN 200

Switch(config)#interface *G 1/0/3*

Switch(config-if)#switch mode access

Switch(config-if)#switch access vlan *200*

Switch(config-if)#exit

Step 6: configure port 1 to Trunk mode and native VLAN to 100

Switch(config)#interface *G 1/0/1*

Switch(config-if)#switch trunk encapsulation *dot1q*

Switch(config-if)#switch mode trunk

Switch(config-if)#switch trunk native vlan *100*

The content of the configuration file **startup_config.conf** that is added to TFTP-SERVER1:

!ROS   Version 3.7.1043.ISCOM2009.84.20080602

!command in view_mode

!

!command in config_mode first-step

create vlan 200 active

!

!command in enable_mode

!

!command in ip igmp profile mode

!

!command in port_mode

Interface port 8

Switch mode trunk

!

!command in vlan configuration mode

!

!command in ip interface mode

interface ip   0

ip address dhcp 200

!

!command in cluster_mode

create vlan 200 active

!

!command in enable_mode

Chapter 31   DHCP Client

This chapter is mainly about how to configure and maintain DHCP Client on the switch, including:

✧ DHCP Client overview

✧ DHCP Client configuration

✧ Monitoring and maintenance

✧ Typical configuration example

✧ DHCP Client trouble shooting

30.1   DHCP client overview

DHCP (Dynamic Host Configuration Protocol) is a protocol to offer client device the configuration information. Based on BOOTP, it adds some function like assigning available network address automatically, network address reuse and other extension configuration. The two protocols can do some interoperation with some mechanism. DHCP offers configuration parameters to the network host, which can be divided into two basic parts: one is offering specific configuration information nto network host, the other part is assigning network address to the host. DHCP is based on client/server mode, where the designated host offers network address and configuration information to the needed host. The designated host is called server.

Usually, DHCP server is used to accomplish IP address assignation in the following situations:

1) Large network scale, it is much too verbose for manual configuration, and cluster management is difficult.

2) In the network the host number is larger than supported IP address number, the system can not offer a static IP address for each host, and the user number access to the network is also limited (for example, Internet service provider is of the situation), lot of users must use DHCP service to get IP address.

3) Only a few hosts need static IP addresses, most hosts do not need that.

There are usually one host and multiple clients (like PC and portable devices) in a typical DHCP application.
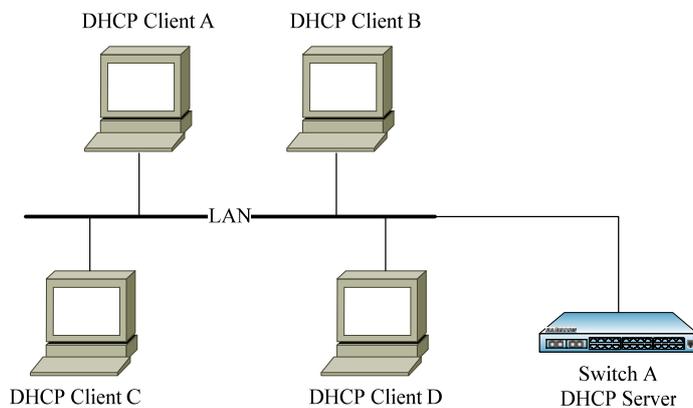

Fig 1-1 Typical DHCP Client application

30.2   Configure DHCP Client

The part is about how to configure DHCP Client on the switch, including:

✧   Default DHCP Client configuration

✧   DHCP Client configuration guide

✧   Configure IP port 0 getting IP address by DHCP

✧   DHCP Client renew

✧   DHCP Client releasing IP address

✧   Configure hostname/class-id/client-id

Attention:

➢   To ISCOM serious devices, the commands related to DHCP Client is under IP port; when it comes to RC551 devices, they are in global configuration mode.

30.2.1 Default DHCP Client configuration

Function	Default value
hostname	raisecomFTTH
class-id	raisecomFTTH-ROS_VERSION
client-id	raisecomFTTH-SYSMAC- IF0
The IP port acquiring IP address by DHCP	N/A
DHCP Client renew	N/A
DHCP Client release IP address	N/A

30.2.2 DHCP Client configuration guide

1. Make sure that DHCP Server or DHCP Relay is not enabled on the switch;

2. To a switch, only IP port 0 supports DHCP Client function;

3. When DHCP Client is enabled, DHCP Server or DHCP Relay can not be enabled on the switch

4. Before using the command, you should make sure that the designated VLAN has been created manually, and the port that IP port lays in has joined the VLAN, while DHCP server has been configured. Or IP address will not be acquired successfully by DHCP.

5. If IP port 0 has been configured acquiring IP address from DHCP, then it not allowed to configure IP address manually under the port.

6. If IP port 0 has acquired IP address form DHCP, run **ip address dhcp** *{1-4094}* **[server-ip ip-address]**, and if the acquired address is different from the designated VLAN or DHCP Server IP address , then the port will release the acquired IP address and start a new application.

7. To port 0, the IP address acquired from DHCP and the manually configured one can cover each

other.

8. If IP port 0 has acquired IP address by DHCP, then it will start IP address renewal automatically.

9. If the client goes through multiple Relay to acquire IP address from DHCP server, make sure that each device is connected and configured correctly. The number of DHCP Relay between the client and server should not exceed 16 in RFC1542, and it is usually recommended not to pass 4.

30.2.3 Configure IP port 0 applying IP address by DHCP

In IP port 0 (only IP port 0), enable DHCP Client, and the device will acquire IP address and requested parameters in the designated VLAN. The parameters includes: gateway address (option 3), TFTP server name (option66), TFTP server address (option 150), configured filename (option 67).

If DHCP server does not support option 150, then you can configure TFTP server address in option 66, which is also supported by DHCP Client.

If one IP address has been configured to IP port 0, then no matter if default gateway configuration successes or not, DHCP Client is thought to have acquired IP address successfully from the server.

The configuration steps are shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip 0**	Enter IP port 0 configuration mode
3	**ip address dhcp** 1	Configure IP port 0 acquiring IP address by DHCP
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp client**	Show DHCP Client configuration and the acquired information (run the command when the application ends)

Attention:

➢ If DHCP Server or DHCP Relay has been enabled on the switch, DHCP Client can not longer be enabled.

➢ If DHCP Client has been enabled on the switch, then DHCP server or DHCP Relay can not be enabled.

30.2.4 DHCP Client renewal

In IP port 0, if IP address has been acquired through DHCP, then you can use the command to renew.

When renewing, the result will be shown in the command lines automatically. If renew successes will be typed out by SYSLOG.

The steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip 0**	Enter IP port 0 configuration mode
3	**ip dhcp client renew**	DHCP Client renew
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp client**	Show DHCP Client configuration and the acquired information (execute the command when renewal ends)

Attention:

➢ The command is available only when IP port 0 has acquired IP address through DHCP.

30.2.5 DHCP Client release IP address

In IP port 0, the steps to release the IP address and other information (like gateway address, TFTP server host name, TFTP server IP address and configured filename) are shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip 0**	Enter IP port 0 configuration mode
3	**no ip address dhcp**	DHCP Client release IP address
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp client**	Show DHCP Client configuration information and the acquired information

Attention:

➢ Only when DHCP Client has been enabled in IP port 0 can the command takes effect.

30.2.6 Configure hostname/class-id/client-id

In IP port 0, configure hostname, class-id and client-id for DHCP Client, which will be used when DHCP Client is sending out messages. Take configuring hostname for example, it is similar when configuring class-id and client-id.

The steps are shown below:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**interface ip 0**	Enter IP port 0 configuration mode
3	**ip dhcp client hostname** *myhost*	Configure hostname to myhost
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp client**	Show DHCP Client configuration and acquired information

Attention:

➢ No matter if DHCP Client has been enabled, hostname, class-id or client-id can be configured. When IP port 0 applies IP address by DHCP Client, current hostname, class-id or client-id is used; when DHCP Client renews, hostname, class-id or client-id should be the same with the one when it is applying IP address.

30.3   Monitoring and maintenance

Use different **show** to show DHCP Client running state and configuration. All the listed **show** commands are shown below:

Command	Description
show ip dhcp client	Show DHCP Client configuration and the acquired information

Use **show ip dhcp client** to show the configuration and acquired information of DHCP Client. The configuration includes: hostname, class-id and client-id. The acquired information includes: the acquired IP address, subnet mask, default gateway, lease length, lease starting and ending time, server address, TFTP server hostname, TFTP server IP address and the configuration filename.

Raisecom#**show ip dhcp client**

Feedback 1: IP port 0 has acquired IP address through DHCP:

```
Hostname:               raisecomFTTH
Class-ID:               raisecomFTTH-3.5.856
Client-ID:               raisecomFTTH-000e5e48e596-IF0

Assigned IP Addr:       10.0.0.5
Subnet mask:            255.0.0.0
Default Gateway:        10.0.0.1
Client lease Starts:    Jan-01-2007 08:00:41
Client lease Ends:       Jan-11-2007 11:00:41
Client lease duration:  874800(sec)
DHCP Server:             10.100.0.1

Tftp server name:       TftpServer
Tftp server IP Addr:    10.168.0.205
```

Startup_config filename: 2109.conf

Feedback 2: IP port 0 is acquiring IP address through DHCP:

Hostname: Raisecom
Class-ID: Raisecom-3.5.856
Client-ID: Raisecom-000e5e48e596-IF0

DHCP Client is requesting for a lease.

Feedback 4: applying IP address fails, no available lease information:

Hostname: Raisecom
Class-ID: Raisecom-3.5.856
Client-ID: Raisecom-000e5e48e596-IF0

No lease information is available.

P.S.:

The blue words, if DHCP Server do not support the option, then replace it with – when showing DHCP Client.

30.4   Typical configuration example

The example is simple but classical on the process of configuring DHCP Client.

1.   Configuration instruction:

The two DHCP clients connect DHCP server by port 2 and 3 respectively.

1)   Configure direct ip pool on DHCP Server, and enable DHCP Server globally.

2)   Configure the two DHCP client acquiring IP address and other configuration information by DHCP.

2.   Topology
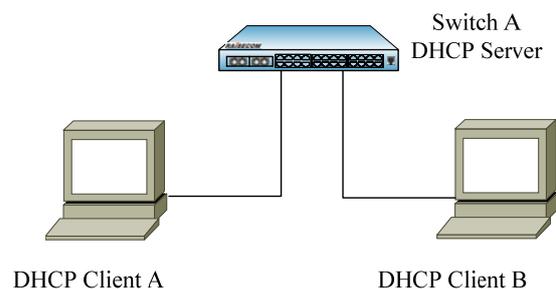
Fig 1-2 Typical configuration example

3.   The configuration steps:

Only the configuration steps of Client A are listed here, the steps of the other one is the same and will not be listed.

➢   Configure IP port 0 acquiring IP address by DHCP:

Raisecom(config)# **interface ip 0**

Raisecom(ip-config)#**ip address dhcp 1**

4. Show

On DHCP Client, use **show ip dhcp client** to show the client IP address applied from DHCP and other configuration information.

Raisecom(config)# **show ip dhcp client**
```
        Hostname:               raisecomFTTH
        Class-ID:               raisecomFTTH-3.6.1025
        Client-ID:               raisecomFTTH-000e5e8a0798-IF0
        Assigned IP Addr:       10.0.0.5
        Subnet mask:            255.0.0.0
        Default Gateway:         10.0.0.1
        Client lease Starts:     Jan-01-2007 08:00:41
        Client lease Ends:       Jan-11-2007 11:00:41
        Client lease duration:   874800(sec)
        DHCP Server:             10.100.0.1

        Tftp server name:        --
        Tftp server IP Addr:     10.168.0.205
        Startup_config filename: 2109.conf
```

30.5   DHCP Client trouble shooting

1. Make sure that DHCP server is able to support option 1, option 3, option 66, option 67, option 150. If some option is not supported, DHCP can not get information of this kind, but for still can get IP address.

2. If the device as DHCP Client starts DHCP Snooping as well, make sure the port it uses to connect DHCP server is the trusted port. Or DHCP Client can not get IP address.

Chapter 32 Optical Module Digital Diagnoses

31.1 Digital diagnoses principle

SFP (Small Form Pluggable) is a kind of optical module in media converter. The fault diagnoses function provides the system a way of performance monitoring. Using the data monitoring function provided by this module, network administrator can forecast the lasting time of the module, insulate the system fault and validate the module compatibility when fixing equipments.

Each SFP module provides five performance parameters: the media converter temperature, inner power supply voltage, sending electronic current, sending optical power and receiving optical power.

The digital diagnoses module polls all the SFP ports every 5 seconds, and gives three datasheet according to the performance parameter getting from the poll: the real-time monitoring table of the optical module, the period performance monitoring table of the optical module, the current period performance monitoring table. When the parameter exceeds the threshold, it will send trap and offer its global switch control.

The index of optical module real-time monitoring table is SFP port number and parameter type. Inside the software the table has stable number of rows, but when you look over it in the command lines only the information of the ports that are active (the row mark is valid) can be shown. Seen from the network management software, the table has stable number of rows, when SFP is not active it means the row mark of the table is invalid. The table restores the parameter value, threshold value, the time and value that the last time the threshold value is exceeded of each parameter for each SFP module. The initialized value of last threshold exceeding is -1000000, the left values are all 0. When the digital diagnose module polls SFP port every 5 seconds, if SFP is active, read SFP's 5 parameter value, adjusting measure, adjusting parameter and threshold value, refresh the parameter value and threshold value of the optical module real-time monitoring table, if it exceeds the threshold value, update the time and value of the exceeding Digital diagnoses configuration. Configure real-time monitoring table that the row mark is invalid. Each row of the table contains 2 variables, which stands for how many 15 minutes' cycle records and 24 hours' cycle records are restored in the parameters of SFP ports. Now digital diagnoses module supports 96 15 minutes' cycle record and 1 24 hours' cycle record at the most.

The index of optical module current period performance monitoring table is SFP port number, period type and parameter type. The table records the maximum value, least value and the average value of the parameters that are within a recording cycle. The table has stable row number, and all the initialized parameter values are 0. When the equipment is started, the digital diagnoses module polls all the SFP ports every 5 seconds, and the value that read first will be evaluated to the maximum, least and average value. Then, if the polling value is larger than the maximum value, refresh it to the larger value; if it is smaller than the least value, refresh the recorded least value, and compute the summation, add 1 on the digit. If SFP is not active when polling, no data record will be refreshed. After 180 polling (15 minutes later), add a row in the period performance monitoring table, and configure the maximum, least and average value of the row's parameter according to current period monitoring table record, cycle type is 15 minutes, then reset all the data in the current period row, and start recording the next cycle. It is the same to record the data of 24 hour cycle. When it reaches 24 hours, add a row in period monitoring table, then reset all the data in the current period row, and

start recording the next cycle.

The index of period performance monitoring table of the optical module is port number, cycle type, cycle recording number and parameter type. The monitoring table restores data of two cycles, that is 15 minutes data and 24 hours data. The table is empty originally. Every 15 minutes, a 15 minutes cycle record will be added to the table. The record number of the newest one is 1, larger recording number means older recording. The table keeps at most 96 fifteen minutes record. When it reaches 96 records, the oldest one will be deleted when a new one is added. Every time it reaches 24 hours, a 24 hour cycle record will be added to the table. The newest recording number is 1, at most 1 twenty-four hour cycle record will be restored in the table, and the old record will be covered every 24 hours.

31.2 Configure digital diagnoses function for optical module

31.2.1 Default digital diagnoses configuration

Function	Default value
Enable/disable sending optical module parameter state unusual trap	Enable sending optical module parameter state unusual trap

31.2.2 Configure optical module parameter state unusual alarm

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp trap transceiver** *{enable|disable}*	Enable/disable sending optical module state unusual trap.
3	**exit**	Return to global configuration mode
4	**show interface transceiver**	Show digital diagnoses information

31.2.3 Optical module digital diagnostic parameter monitoring and maintenance

Commands	Description
show interface port [*port-list]* **transceiver** [*threshold-violations*] [*detail]*	Show digital diagnoses information